05933-049
KUNISA
November 3, 2003

日 本 国 特 許 庁
JAPAN PATENT OFFICE

McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年１１月 ８日

出 願 番 号
Application Number: 特願２００２－３２５８９６

[ST. 10/C]: [ＪＰ２００２－３２５８９６]

出 願 人
Applicant(s): 三洋電機株式会社

２００３年１０月１７日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０８５８５８

【書類名】　特許願

【整理番号】　NQR1020018

【提出日】　平成14年11月 8日

【あて先】　特許庁長官殿

【国際特許分類】　G06T 1/00

G09C 5/00

H04N 1/387

【発明者】

【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内

【氏名】　国狭　亜輝臣

【特許出願人】

【識別番号】　000001889

【氏名又は名称】　三洋電機株式会社

【代理人】

【識別番号】　100105924

【弁理士】

【氏名又は名称】　森下　賢樹

【電話番号】　03-3461-3687

【手数料の表示】

【予納台帳番号】　091329

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子透かし埋め込み装置と方法ならびに電子透かし抽出装置と方法

【特許請求の範囲】

【請求項１】　ホストデータに第１の電子透かしを埋め込む第１の埋め込みブロックと、

前記第１の電子透かしが埋め込まれたホストデータに前記第１の電子透かしの埋め込み位置に関する情報を第２の電子透かしとして埋め込む第２の埋め込みブロックとを含むことを特徴とする電子透かし埋め込み装置。

【請求項２】　前記第１の埋め込みブロックは、

前記第１の電子透かしが埋め込まれるホストデータの埋め込み位置の候補を複数生成する位置情報生成部と、

前記ホストデータの前記埋め込み位置の候補のそれぞれに前記第１の電子透かしを埋め込み、複数の第１の埋め込みホストデータの候補を生成する第１の埋め込み部と、

前記第１の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する第１の評価部と、

前記耐性の評価値に基づいて前記第１の埋め込みホストデータの候補の一つを選択して、前記第１の電子透かしが埋め込まれたホストデータとして出力する第１の選択部とを含むことを特徴とする請求項１に記載の電子透かし埋め込み装置。

【請求項３】　前記第２の埋め込みブロックは、

前記埋め込み位置に関する情報をスクランブルして複数の透かしデータの候補を生成するスクランブル部と、

前記複数の透かしデータの候補をそれぞれ前記第１の電子透かしが埋め込まれたホストデータに埋め込み、複数の第２の埋め込みホストデータの候補を生成する第２の埋め込み部と、

前記第２の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する第２の評価部と、

前記耐性の評価値に基づいて前記第２の埋め込みホストデータの候補の一つを選択して出力する第２の選択部とを含むことを特徴とする請求項１または２に記載の電子透かし埋め込み装置。

【請求項４】　前記第２の埋め込み部は、前記第２の埋め込みホストデータの候補が、前記第１の電子透かしが埋め込まれた後のホストデータからの許容劣化範囲内で、かつ、前記第１の電子透かしが埋め込まれる前の元のホストデータからの許容劣化範囲内に収まるように制限することを特徴とする請求項３に記載の電子透かし埋め込み装置。

【請求項５】　電子透かしが二重に埋め込まれたホストデータから第１の電子透かしを抽出することにより、第２の電子透かしの埋め込み位置に関する情報を取得する第１の抽出ブロックと、

前記ホストデータから前記第１の電子透かしを除去する除去部と、

前記除去部により前記第１の電子透かしが除去されたホストデータから前記埋め込み位置に関する情報にもとづいて前記第２の電子透かしを抽出する第２の抽出ブロックとを含むことを特徴とする電子透かし抽出装置。

【請求項６】　前記第１の抽出ブロックは、電子透かしが二重に埋め込まれた前記ホストデータからスクランブルされた透かしデータを抽出する抽出部と、

前記スクランブルされた透かしデータのスクランブルを解除して、前記第２の電子透かしの埋め込み位置に関する情報を取得するデスクランブル部とを含むことを特徴とする請求項５に記載の電子透かし抽出装置。

【請求項７】　電子透かしが二重に埋め込まれたホストデータの構造であって、第１の電子透かしの埋め込み位置に関する情報が第２の電子透かしとして可逆埋め込み方式により埋め込まれたことを特徴とするコンピュータにて読み取りおよび利用が可能なデータ構造。

【請求項８】　電子透かしが二重に埋め込まれたホストデータから可逆埋め込み方式で埋め込まれた第１の電子透かしを抽出し、その第１の電子透かしを前記ホストデータから除去した上で、第２の電子透かしを抽出することを特徴とする電子透かし抽出方法。

【請求項９】　前記第１の電子透かしは前記第２の電子透かしの透かし方式

を特定するメタ情報であり、前記第２の電子透かしはこのメタ情報で特定される方式で前記ホストデータから抽出されることを特徴とする請求項８に記載の電子透かし抽出方法。

【請求項１０】　電子透かしを二重にホストデータに埋め込む方法であって、第１の電子透かしの埋め込み位置情報を第２の電子透かしとして可逆埋め込み方式により埋め込むことを特徴とする電子透かし埋め込み方法。

【請求項１１】　重要度の異なる情報を含む２つの電子透かしをホストデータに埋め込む方法であって、重要度の高い方の電子透かしの耐性を強化して前記ホストデータに埋め込むことを特徴とする電子透かし埋め込み方法。

【請求項１２】　前記重要度の高い方の電子透かしを可逆埋め込み方式により前記ホストデータに埋め込むことを特徴とする請求項１１に記載の電子透かし埋め込み方法。

【請求項１３】　電子透かしが二重に埋め込まれたホストデータから第１の電子透かしを抽出することにより、第２の電子透かしの埋め込み位置に関する情報を取得する工程と、

前記ホストデータから前記第１の電子透かしを除去する工程と、

前記第１の電子透かしが除去されたホストデータから前記埋め込み位置に関する情報にもとづいて前記第２の電子透かしを抽出する工程とをコンピュータに実行させることを特徴とするコンピュータプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、電子透かし技術に関し、特に電子透かしの埋め込み装置と方法、ならびに電子透かしの抽出装置と方法に関する。

【０００２】

【従来の技術】

ここ数年、インターネット利用人口が急増し、インターネット利用の新たなステージともいえるブロードバンド時代に入ろうとしている。ブロードバンド通信では通信帯域が格段に広がるため、音声、静止画、動画などデータ量の大きいコ

ンテンツの配信も気軽にできるようになる。このようなデジタルコンテンツの流通が盛んになると、コンテンツの著作権の保護がより一層求められることになる。

【０００３】

ネットワーク上に流通するコンテンツのデータは他人に容易にコピーされ、著作権に対する保護が十分ではないのが現状である。そこで著作権を保護するために、コンテンツの作成者や利用者の情報を電子透かしとしてコンテンツデータに埋め込む技術が開発されている。この電子透かし技術を用いることにより、ネットワーク上で流通するコンテンツデータから電子透かしを抽出して、不正利用を検出したり、不正コピーの流通経路を追跡することが可能となる。

【０００４】

従来の電子透かしの埋め込み技術には、電子透かしを埋め込んだ後に、その電子透かしの透かし方式を特定するメタ情報をさらに透かしとして埋め込むものがある（たとえば、特許文献１、特許文献２、および特許文献３参照）。

【０００５】

また、異なる透かし方式を併用したハイブリッド方式によって電子透かしを二重に埋め込むものもある（たとえば、非特許文献１参照）。

【０００６】

【特許文献１】

特開２００２－１６８９１号公報　（全文、第１－５図）

【特許文献２】

特開２０００－２８７０６７号公報　（全文、第１－７図）

【特許文献３】

特開２００１－２５７８６５号公報　（全文、第１－１１図）

【非特許文献１】

大上貴充他、「ハイブリッド式二階層電子透かし方式の提案」、２００２年映像情報メディア学会年次大会、８月、２００２年

【０００７】

【発明が解決しようとする課題】

電子透かしは、不正利用者による改ざんを防止するために、利用者には分からないようにコンテンツデータに埋め込まれる。しかしコンテンツデータは、流通過程や利用過程で、圧縮符号化や各種フィルタリングなどの信号処理が加えられたり、ユーザにより加工されたり、あるいは透かし情報が改ざんされるなど、さまざまな操作を受けることがあり、その過程で埋め込まれた電子透かしデータの一部が変更されたり、消失する可能性がある。したがって電子透かしはこういった操作に対する耐性が要求される。

【０００８】

特許文献１～３では、電子透かしを二重に埋め込み、二重化された透かしを順次抽出する方法が提案されているが、２つの透かしは一般に干渉するため、正しく透かしを検出できない場合が生じる。非特許文献１では、ハイブリッド方式によって電子透かしを二重に埋め込むことにより、２つの透かしの干渉性を軽減しているが、下層の透かし方式が限定されるため、汎用性がない。

【０００９】

本発明はこうした状況に鑑みてなされたもので、その目的は、耐性の強い電子透かしを埋め込み、電子透かしの検出誤差を低減することの可能な技術の提供にある。

【００１０】

【課題を解決するための手段】

本発明のある態様は電子透かし埋め込み装置に関する。この装置は、ホストデータに第１の電子透かしを埋め込む第１の埋め込みブロックと、前記第１の電子透かしが埋め込まれたホストデータに前記第１の電子透かしの埋め込み位置に関する情報を第２の電子透かしとして埋め込む第２の埋め込みブロックとを含む。

【００１１】

ホストデータは、電子透かしを埋め込む対象となるオリジナルデータであり、たとえば静止画、動画、音声などのコンテンツデータである。埋め込まれる電子透かしには、オリジナルデータの識別情報、作成者情報、利用者情報などが含まれる。その他、認証を目的として、ホストデータのダイジェストデータ、すなわちホストデータの特徴を端的に表したデータを電子透かしとして埋め込むことも

可能である。

【００１２】

本発明の別の態様は電子透かし抽出装置に関する。この装置は、電子透かしが二重に埋め込まれたホストデータから第１の電子透かしを抽出することにより、第２の電子透かしの埋め込み位置に関する情報を取得する第１の抽出ブロックと、前記ホストデータから前記第１の電子透かしを除去する除去部と、前記除去部により前記第１の電子透かしが除去されたホストデータから前記埋め込み位置に関する情報にもとづいて前記第２の電子透かしを抽出する第２の抽出ブロックとを含む。

【００１３】

本発明のさらに別の態様は、電子透かしが二重に埋め込まれたホストデータの構造である。このデータ構造は、第１の電子透かしの埋め込み位置に関する情報が第２の電子透かしとして可逆埋め込み方式により埋め込まれた構造を有する。ここで、第１の電子透かしと第２の電子透かしの埋め込まれた順序は任意である。

【００１４】

本発明のさらに別の態様は電子透かし抽出方法に関する。この方法は、電子透かしが二重に埋め込まれたホストデータから可逆埋め込み方式で埋め込まれた第１の電子透かしを抽出し、その第１の電子透かしを前記ホストデータから除去した上で、第２の電子透かしを抽出する。この第２の電子透かしは個別の透かし方式で埋め込まれたものであってもよく、第１の電子透かしは第２の電子透かしの透かし方式を特定するためのメタ情報であり、規格化されたものであってもよい。この場合、第２の電子透かしはこのメタ情報で特定される方式でホストデータから抽出されてもよい。可逆埋め込み方式とは、埋め込み処理の逆変換が可能な方式であり、逆変換により埋め込まれた透かしが完全もしくは完全に近い形で除去される特徴をもつ。

【００１５】

本発明のさらに別の態様は電子透かし埋め込み方法に関する。この方法は、電子透かしを二重にホストデータに埋め込む方法であって、第１の電子透かしの埋

め込み位置情報を第２の電子透かしとして可逆埋め込み方式により埋め込む。ここで、第１の電子透かしと第２の電子透かしの埋め込み順序は任意である。第１の電子透かしの埋め込み後に第２の電子透かしを埋め込んでもよいが、埋め込み順序を逆にして、第１の電子透かしを埋め込む前に、第１の電子透かしの埋め込み位置情報を第２の電子透かしとして埋め込み、その後に第１の電子透かしを埋め込んでもよい。

【００１６】

本発明のさらに別の態様も電子透かし埋め込み方法に関する。この方法は、重要度の異なる情報を含む２つの電子透かしをホストデータに埋め込む方法であって、重要度の高い方の電子透かしの耐性を強化して前記ホストデータに埋め込む。ここでも、重要度の高い方の電子透かしを先に埋め込んでも後に埋め込んでもよい。前記重要度の高い方の電子透かしを可逆埋め込み方式により前記ホストデータに埋め込んでもよい。電子透かしの耐性とは、電子透かしの埋め込まれたホストデータが改変されるなどの攻撃を受けた場合や、埋め込みホストデータに圧縮符号化やフィルタリングなどの信号処理が施された場合など、埋め込みホストデータに対して何らかの操作が加えられた場合に電子透かしデータがもつ頑強性をいう。

【００１７】

なお、以上の構成要素の任意の組み合わせ、本発明の表現を方法、装置、システム、記録媒体、コンピュータプログラムなどの間で変換したものもまた、本発明の態様として有効である。

【００１８】

【発明の実施の形態】

実施の形態１

図１は、実施の形態１に係る電子透かし埋め込み装置１００の構成を示す。実透かし埋め込み部１１２は、入力されたコンテンツＶに実透かしＸを特定の透かし方式によって埋め込み、実透かし埋め込みコンテンツＷを出力する。メタ透かし埋め込み部１２２は、実透かしＸの透かし方式を特定するための実透かし識別情報Ｙ（以下、メタ透かしＹともいう）を実透かし埋め込みコンテンツＷに透か

しとして埋め込み、実透かしＸとメタ透かしＹが埋め込まれた二重透かし埋め込みコンテンツＵを出力する。メタ透かし埋め込み部１２２は、メタ透かしＹを実透かし埋め込みコンテンツＷに埋め込む際、可逆埋め込み方式、すなわち埋め込み処理の逆変換により埋め込まれた透かしを除去して元のデータに復元することができる方式を用いる。

【００１９】

コンテンツＶの著作権を保護するために、コンテンツのＩＤ情報を含む実透かしＸは様々な方式で埋め込むことが許されるが、その埋め込み方式を特定する情報を含むメタ透かしＹは、規格化された共通の方式で埋め込まれる。

【００２０】

図２は、実施の形態１に係る電子透かし抽出装置２００の構成を示す。メタ透かし抽出部２１２は、入力された二重透かし埋め込みコンテンツＵからメタ透かしＹを抽出し、実透かし選択制御部２２２およびメタ透かし除去部２１４に与える。メタ透かし除去部２１４は、メタ透かし抽出部２１２により抽出されたメタ透かしＹを二重透かし埋め込みコンテンツＵから除去し、実透かし埋め込みコンテンツＷを取得して切り替え部２２４に与える。メタ透かしＹは可逆埋め込み方式によって埋め込まれているため、メタ透かし除去部２１４は、埋め込み時の処理の逆変換を行うことによって、二重透かし埋め込みコンテンツＵをメタ透かしＹを埋め込む前の状態、すなわち実透かし埋め込みコンテンツＷに復元することが可能である。

【００２１】

実透かし選択制御部２２２は、メタ透かし抽出部２１２により抽出されたメタ透かしＹにより、実透かしＸの透かし方式を特定し、特定された透かし方式の識別情報を切り替え部２２４に与える。切り替え部２２４は、特定の透かし方式ごとに用意された複数の特定実透かし抽出部２２６の内、実透かし選択制御部２２２により与えられた透かし方式の識別情報にもとづいて、その透かし方式に合ったいずれかの特定実透かし抽出部２２６を選択し、メタ透かし除去部２１４から供給される実透かし埋め込みコンテンツＷをその選択された特定実透かし抽出部２２６に供給するように切り替える。

【００２２】

特定実透かし抽出部２２６は、特定の透かし方式にもとづいて透かしを抽出する機能を有し、メタ透かし除去部２１４から供給された実透かし埋め込みコンテンツＷからその特定の透かし方式により実透かしＸを抽出して出力する。

【００２３】

本実施の形態によれば、電子透かし抽出装置２００において、メタ透かし除去部２１４がメタ透かしＹを除去した上で、実透かしＸが抽出されるので、実透かしＸとメタ透かしＹの干渉による検出精度の劣化を防ぐことができる。

【００２４】

本実施の形態の電子透かし抽出装置２００は、たとえばコンテンツを提供するサーバなどに設置して、様々な透かし方式により透かしが埋め込まれたコンテンツをユーザに提供するために用いられてもよい。電子透かし抽出装置２００は、ユーザからコンテンツの要求があったとき、メタ透かしを抽出して、透かし方式を特定して実透かしを抽出し、実透かしに含まれるコンテンツの利用条件などを照合して、ユーザにコンテンツの利用を許諾することができる。

【００２５】

実施の形態２

図３は、実施の形態２に係る電子透かし埋め込み装置１００の構成を示す。第１透かし埋め込み部１１４は、入力されたコンテンツＶに第１透かしＸを埋め込み、第１透かし埋め込みコンテンツＷを出力し、第１透かしＸの埋め込み位置情報Ｙを第２透かし埋め込み部１２４に与える。

【００２６】

第１透かし埋め込み部１１４は、コンテンツＶの特徴量にもとづいて第１透かしＸを埋め込む位置を決める。たとえばコンテンツＶが画像データである場合、ピクセル値の分布などを評価して透かしを埋め込んでも目立たない位置を選んだり、エッジ部など画像の高周波成分を埋め込み位置として選んだり、あるいは画像圧縮などの処理に対する耐性を考慮して埋め込み位置を選んだりして、不可視性や耐性を考慮した埋め込み位置を決定する。したがって埋め込み位置はそれぞれのコンテンツＶによって異なる。

【００２７】

第２透かし埋め込み部１２４は、第１透かし埋め込み部１１４から与えられた埋め込み位置情報Ｙ（以下、第２透かしＹともいう）を第１透かし埋め込みコンテンツＷに埋め込み、第１透かしＸと第２透かしＹが埋め込まれた二重透かし埋め込みコンテンツＵを出力する。なお、第２透かし埋め込み部１２４は、可逆埋め込み方式により第２透かしＹを第１透かし埋め込みコンテンツＷに埋め込む。

【００２８】

図４は、実施の形態２に係る電子透かし抽出装置２００の構成を示す。第２透かし抽出部２１６は、入力された二重透かし埋め込みコンテンツＵから第２透かし、すなわち埋め込み位置情報Ｙを抽出し、第１透かし抽出部２２８および第２透かし除去部２１８に与える。第２透かし除去部２１８は、埋め込み処理の逆変換を行って、第２透かしＹを二重透かし埋め込みコンテンツＵから除去し、第１透かし埋め込みコンテンツＷを取得して第１透かし抽出部２２８に与える。

【００２９】

第１透かし抽出部２２８は、第２透かし抽出部２１６により抽出された埋め込み位置情報Ｙをもとに透かしの埋め込み位置を特定し、第１透かし埋め込みコンテンツＷから第１透かしＸを抽出して出力する。

【００３０】

本実施の形態によれば、透かしの埋め込み位置が第２の透かしとしてコンテンツに埋め込まれるため、透かしの埋め込み位置を秘密鍵で提供したり、コンテンツのヘッダに含めて提供するなど、透かしの埋め込み位置を利用者に知らせるための処理が不要になる。

【００３１】

実施の形態３

図５は、実施の形態３に係る電子透かし埋め込み装置１００の構成を示す。この構成は、ハードウエア的には、任意のコンピュータのＣＰＵ、メモリ、その他のＬＳＩで実現でき、ソフトウエア的にはメモリにロードされた電子透かし埋め込み機能のあるプログラムなどによって実現されるが、ここではそれらの連携によって実現される機能ブロックを描いている。したがって、これらの機能ブロッ

クがハードウエアのみ、ソフトウエアのみ、またはそれらの組み合わせによっていろいろな形で実現できることは、当業者には理解されるところである。

【００３２】

電子透かし埋め込み装置１００は、第１透かし埋め込みブロック１１０と第２透かし埋め込みブロック１２０を含む。第１透かし埋め込みブロック１１０は、ホストデータＶに透かし情報Ｉを埋め込む処理を行い、第１埋め込みホストデータＷを出力する。第２透かし埋め込みブロック１２０は、透かし情報Ｉの埋め込み位置に関する情報を第１埋め込みホストデータＷに第２透かしとして埋め込む処理を行い、第２埋め込みホストデータＵを出力する。

【００３３】

ここで、ホストデータＶは、たとえば音声、静止画、動画などのデータである。透かし情報Ｉは、そのホストデータＶの識別情報、作成者情報、利用者情報など著作権に関する情報、ホストデータＶの改ざん検出を行う認証情報、タイムスタンプなどである。

【００３４】

第１透かし埋め込みブロック１１０は、第１透かしデータＸをホストデータＶの複数の埋め込み位置の候補に埋め込み、透かしの耐性が強くなる候補を選択して、最終的な第１埋め込みホストデータＷとして出力する。暗号化部１０は、ホストデータＶに埋め込むべき透かし情報Ｉを秘密鍵Ｋにより暗号化し、第１透かしデータＸを出力する。透かし情報の暗号化を行わない場合には、暗号化部１０の構成は省略してもよい。

【００３５】

位置検出部１２は、ホストデータＶの特徴と秘密鍵Ｋにもとづいて第１透かしデータＸの埋め込み位置Ｐを決定し、第１透かし埋め込み部１４は、秘密鍵Ｋを用いて、ホストデータＶの埋め込み位置Ｐに第１透かしデータＸを埋め込み、第１埋め込みホストデータＷを出力する。図５では、暗号化部１０、位置検出部１２、第１透かし埋め込み部１４、第２透かし埋め込みブロック１２０の変更部１６および第２透かし埋め込み部１８に秘密鍵Ｋの情報が入力されているが、各部に入力される秘密鍵Ｋの情報はお互いに独立であってもよい。また、秘密鍵Ｋの

情報の一部が従属する内容であってもよく、完全に同一のものであってもよい。さらには、秘密鍵Ｋに依存しない埋め込み方式を採用してもよい。位置検出部１２と埋め込み部１４は協同して、複数の埋め込み位置Ｐを生成し、それぞれの埋め込み位置Ｐに第１透かしデータＸを埋め込み、複数の埋め込みホストデータＷの候補を生成し、それらの候補の一つを選択する機能をもつ。

【００３６】

第２透かし埋め込みブロック１２０は、第１透かしデータＸの埋め込み位置Ｐの識別情報を含む第２透かしデータＹをスクランブルして、第１埋め込みホストデータＷに埋め込み、第２埋め込みホストデータＵを出力する。変更部１６は、第２透かしデータＹ、第１埋め込みホストデータＷ、および秘密鍵Ｋを用いて、第２透かしデータＹをスクランブルし、スクランブルされた第２透かしデータＹ’を出力する。

【００３７】

第２透かし埋め込み部１８は、秘密鍵Ｋを用いて、スクランブルされた透かしデータＹ’を第１埋め込みホストデータＷに埋め込み、第２埋め込みホストデータＵを出力する。秘密鍵Ｋに依存しない埋め込み方式を用いてもよい。

【００３８】

変更部１６と第２透かし埋め込み部１８は協同して、複数のスクランブルされた透かしデータＹ’を生成し、それぞれを第２埋め込みホストデータＷに埋め込み、複数の第２埋め込みホストデータＵの候補を生成し、それらの候補の一つを選択する機能をもつ。

【００３９】

図６は第１透かし埋め込みブロック１１０の位置検出部１２および第１透かし埋め込み部１４の機能構成図である。ＥＣＣ（Error Correction Code）部２４は第１透かしデータＸに誤り訂正のためのパリティを付加した透かしデータX_cを生成する。ＥＣＣ部２４は、透かしビットの検出率を向上させるためのオプションであって、アプリケーションによっては必要ない場合もあり、この構成を省略してもよい。

【００４０】

位置情報生成部６０は、ホストデータＶについてＬ$_1$個の埋め込み位置Ｐの候補をランダムに生成する。第１埋め込み部２６はＬ$_1$個の埋め込み位置Ｐの候補のそれぞれに透かしデータＸ$_c$を埋め込み、Ｌ$_1$種類の第１埋め込みホストデータＷの候補を生成する。

【００４１】

Ｌ$_1$個のＳＮＲ計算部２８は、Ｌ$_1$種類の第１埋め込みホストデータＷの候補のそれぞれについて、第１透かしデータＸの耐性を評価する。セレクタ３２は、耐性の評価値が最良である第１埋め込みホストデータＷの候補を選択し、それを最終的な第１埋め込みホストデータＷとして出力し、その場合の第１透かしデータＸの埋め込み位置情報Ｐ＊を出力する。

【００４２】

埋め込み位置の候補は、一例としてテーブルマッチングによりランダムに生成される。位置情報生成部６０は、埋め込み位置の候補を識別するための識別情報と埋め込む位置とを対応づけたテーブルを備え、このテーブルを参照して、埋め込み位置の候補の識別データに対応づけて埋め込み位置の候補を生成する。このテーブルは、透かしデータの第１ビットについて、たとえば、「識別番号０の場合は（１，２９）の位置、識別番号１の場合は（９８３，２５１）の位置、・・・、識別番号１５の場合は（５４２，３７）の位置に埋め込む」といった識別番号と埋め込み座標との対応関係を格納する。第２番目から第ｎ$_1$番目のビットについてもそれぞれ埋め込み位置が異なる対応関係が格納される。埋め込み位置は何らかの方法でランダムに生成されたものである。

【００４３】

図７は第２透かし埋め込みブロック１２０の変更部１６および第２透かし埋め込み部１８の機能構成図である。第２透かし埋め込みブロック１２０は第１透かし埋め込みブロック１１０から第１埋め込みホストデータＷと埋め込み位置情報Ｐ＊を供給される。埋め込み位置情報Ｐ＊は、第１透かしデータＸの各ビットの埋め込み位置の識別情報であり、この識別情報を含む透かしビットの系列を第２透かしデータＹと表記する。Ｌ$_2$個のマルチプレクサ２０は、第２透かしデータＹの先頭にそれぞれ初期データＣ$_0$～Ｃ$_{Ｌ2－1}$を挿入したＬ$_2$種類のビット系

列Ｙ$_b$を生成する。Ｌ$_2$個のスクランブラ２２はＬ$_2$種類のビット系列をそれぞれスクランブルして、Ｌ$_2$種類のスクランブルされた透かしデータＹ’$_b$を生成する。Ｌ$_2$個のＥＣＣ部２４はＬ$_2$種類のスクランブルされた透かしデータＹ’$_b$のそれぞれに誤り訂正のためのパリティを付加した透かしデータＹ’$_c$を生成する。

【００４４】

Ｌ$_2$個の第２埋め込み部２７は、可逆埋め込み方式により、Ｌ$_2$種類のスクランブルされた透かしデータＹ’$_c$のそれぞれを第１埋め込みホストデータＷに埋め込み、Ｌ$_2$種類の第２埋め込みホストデータＵの候補を生成する。Ｌ$_2$個のＳＮＲ計算部２８は、Ｌ$_2$種類の第２埋め込みホストデータＵの候補のそれぞれについて、透かしデータＹの耐性を評価する。セレクタ３０は、耐性の評価値が最良である第２埋め込みホストデータＵの候補を選択し、それを最終的な第２埋め込みホストデータＵとして出力する。

【００４５】

図８は、実施の形態３に係る電子透かし抽出装置２００の構成を示す。電子透かし埋め込み装置１００により電子透かしが埋め込まれた第２埋め込みホストデータＵは、ネットワーク上で流通し、コンピュータにおいて利用される。その過程で第２埋め込みホストデータＵは圧縮符号化や改ざんなどの操作を受ける。画像データであれば、ＪＰＥＧ圧縮、フィルタリング、量子化、色補正などの信号処理や、スケーリング、クロッピング、回転、並行移動等の幾何学的な変換など有用性のある操作が施されたり、電子透かしを除去したり改変するなどの不正な攻撃が加えられたりする。そのような操作による変形を第２埋め込みホストデータＵに対するノイズＮとみなし、ノイズＮが付加した第２埋め込みホストデータＵを第２埋め込みホスト信号Ｕ＾（＝Ｕ＋Ｎ）とする。電子透かし抽出装置２００は、第２埋め込みホスト信号Ｕ＾から埋め込まれた透かしデータＸを抽出する処理を行う。

【００４６】

電子透かし抽出装置２００は、第２透かし抽出ブロック２１０と第１透かし抽出ブロック２２０を含む。第２透かし抽出ブロック２１０は、第２埋め込みホス

ト信号Ｕ＾から第２透かしデータＹを抽出する処理を行う。第２抽出部４０は、秘密鍵Ｋを用いて、第２埋め込みホスト信号Ｕ＾に埋め込まれた第２透かしデータＹ＾$_c$を抽出する。ＥＣＣ復号部４４はこの第２透かしデータＹ＾$_c$に付加されているパリティビットを用いて誤り訂正を行い、第２透かしデータＹ＾$_b$を生成する。デスクランブラ４６は秘密鍵Ｋを用いて、誤り訂正後の第２透かしデータＹ＾$_b$のスクランブルを解除し、先頭部の初期データを取り除いて第２透かしデータＹ＾を出力する。この第２透かしデータＹ＾には第１透かしデータＸの埋め込み位置情報Ｐ＾が含まれ、この埋め込み位置情報Ｐ＾は電子透かし抽出装置２００の第１抽出部４８に供給される。

【００４７】

第２透かし抽出ブロック２１０の第２透かし除去部４２は、図７の第２透かし埋め込みブロック１２０の第２埋め込み部２７の埋め込み処理の逆変換を行うことにより、第２抽出部４０により抽出された第２透かしデータＹ＾$_c$を第２埋め込みホスト信号Ｕ＾から除去し、第１埋め込みホスト信号Ｗ＾を出力する。

【００４８】

第１透かし抽出ブロック２２０は、第２透かし抽出ブロック２１０の第２透かし除去部４２から供給される第１埋め込みホスト信号Ｗ＾から第１透かしデータＸを抽出する処理を行う。第１抽出部４８は、第２透かし抽出ブロック２１０のデスクランブラ４６が出力する第２透かしデータＹ＾から埋め込み位置情報Ｐ＾を取得し、秘密鍵Ｋを用いて、第２透かし抽出ブロック２１０の第２透かし除去部４２から得た第１埋め込みホスト信号Ｗ＾から埋め込み位置情報Ｐ＾で示される位置に埋め込まれた第１透かしデータＸ＾$_c$を抽出する。ＥＣＣ復号部４５は、この第１透かしデータＸ＾$_c$に付加されているパリティビットを用いて誤り訂正を行い、第１透かしデータＸ＾$_b$を生成して出力する。

【００４９】

第１抽出部４８は、一例として前述のテーブルマッチングの方法を用い、図６の位置情報生成部６０が参照するテーブルと同じデーブルを参照して、埋め込み位置情報Ｐ＾にもとづき、埋め込み位置の識別情報情報に対応づけられた埋め込み位置を特定し、第１透かしデータＸ＾をその位置から抽出する。

【００５０】

なお、上記の説明では、図７で示したように、L_2種類の透かしデータの候補を生成するために、L_2個のマルチプレクサ２０、スクランブラ２２、ＥＣＣ部２４、第２埋め込み部２７、およびＳＮＲ計算部２８が並列に設けられたが、これらの部材を単一構成にして、L_2種類の透かしデータの候補を逐次的に生成、評価して最適な候補を選択してもよい。透かしデータの候補を逐次生成し、埋め込み強度が所望の基準値以上である候補が得られた時点で、その候補を最終的な埋め込みホストデータＷとして選択し、そのような候補が生成されなければ、L_2個の埋め込みホストデータの候補の中から埋め込み強度が最大であるものを最終的な埋め込みホストデータＷとして選択することができる。

【００５１】

以上の構成の電子透かし埋め込み装置１００および電子透かし抽出装置２００による電子透かしの埋め込みと抽出の手順を説明する。

【００５２】

（１）第１透かしデータＸの埋め込み手順

図９は、電子透かし埋め込み装置１００の第１透かし埋め込みブロック１１０による第１透かしデータＸの埋め込み手順を説明するフローチャートである。位置情報生成部６０は、第１透かしデータＸのL_1個の埋め込み位置候補P^k（$k=0, \cdots, L_1-1$）を生成する（Ｓ３０）。

【００５３】

ＥＣＣ部２４は、第１透かしデータＸに誤り訂正のためのパリティを付加し、第１埋め込み部２６は、ホストデータＶのL_1個の埋め込み位置の候補P^kのそれぞれに第１透かしデータＸを埋め込む（Ｓ３２）。

【００５４】

第１透かしデータＸは次のようにn_1ビットのビット系列で表される。

$X=\{x_0, x_1, \cdots, x_{n1-1}\}$

このn_1ビットの第１透かしデータＸの埋め込み位置の候補P^kに対応するホストデータＶのサンプルの集合のペア（$V+k$，$V-k$）を次のように定義する。サンプルの集合$V+k$，$V-k$はそれぞれn_1個の要素をもつ。なお、ホストデ

ータＶは、空間軸上のサンプル、時間軸上のサンプル、周波数軸上のサンプル、たとえばＤＣＴ変換、ＦＦＴ変換、ＤＷＴ変換などの処理後のサンプルなどにより表現される。

【００５５】

$V+k=\{v+k_0, v+k_1, \cdots, v+k_{n1-1}\}$

$V-k=\{v-k_0, v-k_1, \cdots, v-k_{n1-1}\}$

ここでサンプルの集合$V+k$，$V-k$の要素である各サブセット$v+k_i$、$v-k_i$は、次のようにホストデータＶのm_1個のサンプルデータからなる。

$v+k_i=\{v+k_i, 0, v+k_i, 1, \cdots, v+k_i, m1-1\}$

$v-k_i=\{v-k_i, 0, v-k_i, 1, \cdots, v-k_i, m1-1\}$

【００５６】

第１透かしデータＸの各ビットを埋め込み位置の候補P^kに対応したL_1個のサンプルの集合のペア（$V+k$，$V-k$）に次のように埋め込み、L_1種類の第１埋め込みホストデータの候補W^kを生成する。

【００５７】

$w+k_{i,j}=v+k_{i,j}+\alpha+_{i,j}\cdot x_i$

$w-k_{i,j}=v-k_{i,j}-\alpha-_{i,j}\cdot x_i$

ここで$\alpha+_{i,j}$および$\alpha-_{i,j}$は人間の視覚モデルにもとづいて知覚されるノイズを減少するためのスケーリングパラメータであり、いずれも正の値である。あるいは、$\alpha+_{i,j}$および$\alpha-_{i,j}$は、ある確率分布、たとえばガウシアン分布、一様分布などに従うように、秘密鍵Ｋによって生成される正の値であってもよい。この場合、透かしの埋め込み強度は減少するが、埋め込まれた透かしの秘匿性は向上する。

【００５８】

このようにして、第１透かしデータの各ビットx_iは各サブセット$v+k_i$、$v-k_i$のそれぞれm_1個のサンプルに重複して埋め込まれる。重複の数m_1が大きいほど、透かしビットが失われる可能性が低くなり、検出誤差が小さくなる一方で、ホストデータに埋め込むことができる透かしのビット数が減少する。$\alpha+_{i,j}$および$\alpha-_{i,j}$は、視覚上の劣化を検知できないようにピクセル毎に

設定される値であり、原理的には、埋め込むピクセル数m_1を増やしても、人間の視覚上、画質の劣化は検知されない。しかし、１ビットを埋め込むのに費やすピクセル数が増加するということは、埋め込み領域には制限があるため、埋め込むことができるビット数が減少することを意味し、したがって埋め込み率の低下を招くことなる。

【００５９】

ＳＮＲ計算部２８は、L_1種類の第１埋め込みホストデータの候補W^kに対して第１透かしデータＸの耐性、すなわち埋め込み強度を評価し（Ｓ３４）、セレクタ３２は埋め込み強度が最大となる第１埋め込みホストデータの候補W^kを最終的な第１埋め込みホストデータＷとして選択する（Ｓ３６）。

【００６０】

埋め込み強度の評価は、ホストデータＶを第１透かしデータＸに対するノイズとみなして、埋め込まれた透かしデータＸに対して検出される透かしデータの分散を計算することにより行われる。分散が小さいほど、耐性が強いと考えることができる。第１埋め込みホストデータの候補のペア（W^{+k}，W^{-k}）に対して次式によりＳＮ比を評価して、最適な候補Ｋを選択する。

【００６１】

$$K=\mathrm{argmax}_k\left(P_k/\sigma_k^2\right)$$

$$P_k=\Sigma_{i=0}^{n1-1}\left|\Sigma_{j=0}^{m1-1}\left(w^{+k}{}_{i,j}-w^{-k}{}_{i,j}\right)\right|^2/n$$

$$\sigma_k^2=\Sigma_{i=0}^{n1-1}\left|\Sigma_{j=0}^{m1-1}\left(w^{+k}{}_{i,j}-w^{-k}{}_{i,j}\right)-P_k{}^{1/2}\cdot w_i\right|^2/n$$

【００６２】

（２）第２透かしデータＹの埋め込み手順

図１４は、電子透かし埋め込み装置１００の第２透かし埋め込みブロック１２０による第２透かしデータＹの埋め込み手順を説明するフローチャートである。フローチャートの説明にあたり、図１０から図１３を適宜参照する。

【００６３】

第２透かし埋め込みブロック１２０は第１透かし埋め込みブロック１１０から

第１透かしデータＸの埋め込み位置情報Ｐ＊を得る。マルチプレクサ２０は、この埋め込み位置情報Ｐ＊を識別情報として含む第２透かしデータＹの先頭に$Ｌ_2$種類の初期データを挿入して$Ｌ_2$個の符号系列を生成し（Ｓ１０）、スクランブラ２２は、それらの符号系列をスクランブルして$Ｌ_2$種類のスクランブルされた第２透かしデータＹ’を生成する（Ｓ１２）。

【００６４】

図１０は、第２透かしデータＹと$Ｌ_2$種類のスクランブルされた第２透かしデータＹ’との関係を示す。$ｎ_2$ビットの第２透かしデータＹの先頭に、$ｒ_2$ビットの冗長語を識別データＩＤ［０］～ＩＤ［$Ｌ_2$－１］として付加し、$Ｌ_2$種類の第２透かしデータの候補を作成する。最大$２^{ｒ_2}$種類の候補が作成される。これらの候補に含まれる第２透かしデータＹのビット列はこれから述べるスクランブル方式により、スクランブルされる。

【００６５】

スクランブル方式の一例として、伝送や磁気記録におけるデジタル変調の際に利用されるＧＳ（Guided Scramble）方式を採用する。ＧＳ方式は、ある一定のデータブロック長からなる情報系列に対して、Ｌ種類の符号系列を生成し、これらを次に送信する符号系列の候補として扱う。これらの候補の中から、伝送媒体の性質に合わせて最適なものを選択して最終的な符号系列とする。このＧＳ方式により、多様性に富んだ符号系列の候補を簡単な方法で生成することができる。

【００６６】

第２透かし埋め込みブロック１２０におけるマルチプレクサ２０とスクランブラ２２がＧＳ符号化器の一部として機能する。ＧＳ符号化器は、ｎビットからなる情報系列Ｄ（ｘ）の直前にＬ種類のｒビットの冗長語$ｃ_i$（ｉ＝０，・・・，Ｌ－１）を付加し、Ｌ種類の符号系列$ｃ_i x^n＋Ｄ（ｘ）$を生成する。この符号系列の符号長は（ｎ＋ｒ）ビットとなる。このようにして冗長語が付加された符号系列に対して、次式のようにＮ次元のスクランブル多項式Ｓ（ｘ）で除算することにより商$Ｔ_i$（ｘ）を求める。

【００６７】

$$Ｔ_i（ｘ）＝Ｑ_Ｓ（ｘ）［（ｃ_i x^n＋Ｄ（ｘ））x^N］　　（１）$$

ただし、Ｑａ［ｂ］はｂをａで除算した商を示す。商集合｛Ｔ０（ｘ），・・・，ＴＬ－１（ｘ）｝がスクランブル後の符号系列の候補である。これらの候補の各々について、その符号系列が実際に用いられた際の性能を評価し、その評価値が最良であるものを最終的な符号系列として選択する。

【００６８】

透かし抽出時には、第２透かし抽出ブロック２１０におけるデスクランブラ４６がＧＳ復号器として機能し、符号系列にＳ（ｘ）を乗算し、下位Ｎビットと上位ｒビットの変換情報を捨てることにより、元の情報系列Ｄ（ｘ）が得られる。

【００６９】

ここでスクランブル多項式Ｓ（ｘ）として、Ｓ（ｘ）＝ｘ^{r}＋１を用いた場合を説明する。ｎ　ｍｏｄ　ｒ＝０の場合、（１）式は次式に示す畳み込み演算で表現可能である。

【００７０】

$t_j = d_j$（＋）c_i　（ｊ＝０）

$t_j = d_j$（＋）t_{j-1}　（ｊ＝１，・・・，ｎ／ｒ－１）

ただし、ｉ＝０，・・・，Ｌ－１であり、d_jは元の情報系列Ｄ（ｘ）をｒビットずつ区切ったビット列、t_jは変換後の符号系列T_i（ｘ）の先頭のｒビットの冗長語c_i以降をｒビットずつ区切ったビット列である。また（＋）は排他的論理和（ＥＸ－ＯＲ）演算を示す。

【００７１】

図１１はこの透かし埋め込み時の畳み込み演算を説明する図である。たとえば、ｎ＝６、ｒ＝２の場合を考える。元の情報系列Ｄ（ｘ）＝（１，０，１，０，０，１）に対して、冗長語c_0＝（０，０）を付加して、変換後の符号系列T_0（ｘ）を生成する。上記の符号化時の畳み込み演算により、$t_0 = d_0$（＋）c_0＝（１，０）（＋）（０，０）＝（１，０）、$t_1 = d_1$（＋）t_0＝（１，０）（＋）（１，０）＝（０，０）、$t_2 = d_2$（＋）t_1＝（０，１）（＋）（０，０）＝（０，１）となり、変換後の符号系列T_0＝（０，０，１，０，０，０，０，１）が得られる。ここで変換後の符号系列T_0の先頭の２ビットは冗長語c_0であることに注意する。

【００７２】

同様にして、冗長語c_1＝（０，１）、c_2＝（１，０）、c_3＝（１，１）に対して、それぞれ変換後の符号系列T_1＝（０，１，１，１，０，１，０，０）、T_2＝（１，０，０，０，１，０，１，１）、T_3＝（１，１，０，１，１，１，１，０）が得られる。

【００７３】

透かし抽出時は次式のように畳み込み演算を行うことにより、元の情報系列Ｄ（ｘ）が得られる。

【００７４】

$d_j = t_j (+) c_i$　（ｊ＝０）

$d_j = t_j (+) t_{j-1}$　（ｊ＝１，・・・，ｎ／ｒ－１）

【００７５】

図１２はこの透かし抽出時の畳み込み演算を説明する図である。前述の例において、変換後の符号化系列T_0＝（０，０，１，０，０，０，０，１）が与えられると、先頭の２ビットから冗長語c_0＝（０，０）が得られ、上記の復号時の畳み込み演算により、$d_0 = t_0 (+) c_0$＝（１，０）（＋）（０，０）＝（１，０）、$d_1 = t_1 (+) t_0$＝（０，０）（＋）（１，０）＝（１，０）、$d_2 = t_2 (+) t_1$＝（０，１）（＋）（０，０）＝（０，１）となり、元の情報系列Ｄ（ｘ）＝（１，０，１，０，０，１）が得られる。他の変換後の符号化系列T_1，T_2，T_3についてもこの畳み込み演算により、元の情報系列Ｄ（ｘ）が得られる。

【００７６】

再び図１４を参照する。スクランブラ２２によって生成されたL_2種類のスクランブルされた透かしデータＹ’は、ＥＣＣ部２４により誤り訂正のためのパリティを付加された後に、第２埋め込み部２７により第１埋め込みホストデータＷに埋め込まれる（Ｓ１４）。

【００７７】

図１３（ａ）、（ｂ）は、スクランブルされた透かしデータＹ’の埋め込み方法を説明する図である。L_2種類のスクランブルされた透かしデータＹ’をy_0

，$y_{,1}$，・・・，y_{L2-1}とする。各透かしデータの候補のビット系列は、次式のように表される。先頭のr_2ビットは識別データである。また、スクランブル処理後のビット０は、－１に置き換えて、以下の処理を行う。

【００７８】

$y^0=\{-1,\cdots,-1,-1,y^0{}_0,y^0{}_1,\cdots,y^0{}_{n2-1}\}$

$y^1=\{-1,\cdots,-1,1,y^1{}_0,y^1{}_1,\cdots,y^1{}_{n2-1}\}$

・・・

$y_{L2-1}=\{1,\cdots,1,1,y_{L2-1}{}_0,y_{L2-1}{}_1,\cdots,y_{L2-1}{}_{n2-1}\}$

【００７９】

（n_2+r_2）ビットの透かしデータＹの埋め込み対象として選択された第１埋め込みホストデータＷから、第２透かし埋め込み用の秘密鍵を用いて、サンプル集合のペア（Ω^+，Ω^-）を次のように選択する。このサンプル集合（Ω^+，Ω^-）は第１埋め込みホストデータＷから第２透かし埋め込み用の秘密鍵にもとづいて選択される集合であり、第１透かしデータＸの埋め込み対象として第１透かし埋め込み用の秘密鍵にもとづいて選択されたサンプル集合（V^+，V^-）とは独立に選択される。したがって、第１透かし埋め込み後のサンプル集合（W^+，W^-）とは区別する意味で、ここでは第２透かしの埋め込み対象のサンプル集合を（Ω^+，Ω^-）と表記している。サンプルの集合Ω^+，Ω^-は次のようにそれぞれ（n_2+r_2）個の要素をもつ。なお、第１埋め込みホストデータＷは、空間軸上のサンプル、時間軸上のサンプル、周波数軸上のサンプル、たとえばＤＣＴ変換、ＦＦＴ変換、ＤＷＴ変換などの処理後のサンプルなどにより表現される。

【００８０】

$\Omega^+=\{\omega^+{}_0,\omega^+{}_1,\cdots,\omega^+{}_{n2+r2-1}\}$

$\Omega^-=\{\omega^-{}_0,\omega^-{}_1,\cdots,\omega^-{}_{n2+r2-1}\}$

ここでサンプルの集合Ω^+，Ω^-の要素である各サブセット$\omega^+{}_i$、$\omega^-{}_i$は、次のように第１埋め込みホストデータＷのm_2個のサンプルデータからなる。

【００８１】

$\omega^{+}{}_{i} = \{\omega^{+}{}_{i,0}, \omega^{+}{}_{i,1}, \cdots, \omega^{+}{}_{i,m2-1}\}$

$\omega^{-}{}_{i} = \{\omega^{-}{}_{i,0}, \omega^{-}{}_{i,1}, \cdots, \omega^{-}{}_{i,m2-1}\}$

【００８２】

第２透かしデータの候補y^{k}（$k=0, \cdots, L_2-1$）をサンプルの集合のペア（Ω^{+}, Ω^{-}）に次のように埋め込み、L_2種類の第２埋め込みホストデータの候補U^{k}を生成する。

【００８３】

$u^{+k}{}_{i,j} = \omega^{+}{}_{i,j} + \beta^{+}{}_{i,j} \cdot y^{k}{}_{i}$

$u^{-k}{}_{i,j} = \omega^{-}{}_{i,j} - \beta^{-}{}_{i,j} \cdot y^{k}{}_{i}$

ここで$\beta^{+}{}_{i,j}$および$\beta^{-}{}_{i,j}$は人間の視覚モデルにもとづいて知覚されるノイズを減少するためのスケーリングパラメータであり、いずれも正の値である。あるいは、$\beta^{+}{}_{i,j}$および$\beta^{-}{}_{i,j}$は、ある確率分布、たとえばガウシアン分布、一様分布などに従うように、秘密鍵Ｋによって生成される正の値であってもよい。このようにして、ｋ番目の第２透かしデータの候補の各ビット$y^{k}{}_{i}$は各サブセット$\omega^{+}{}_{i}$、$\omega^{-}{}_{i}$のそれぞれm_2個のサンプルに重複して埋め込まれる。

【００８４】

各サブセット$\omega^{+}{}_{i}$、$\omega^{-}{}_{i}$は、一例として、特定のＤＣＴ（Discrete Cosine Transform）ブロックを示しており、透かしビットの埋め込み対象として選ばれるm_2個のサンプルデータは、そのＤＣＴブロックに含まれるm_2個のＤＣＴ係数である。図１３（ａ）、（ｂ）は、８×８のＤＣＴブロックのペア$\omega^{+}{}_{i}$、$\omega^{-}{}_{i}$のそれぞれm_2個のＤＣＴ係数に第２透かしデータ$y^{k}{}_{i}$が埋め込まれる様子を示している。ブロックペア$\omega^{+}{}_{i}$、$\omega^{-}{}_{i}$およびm_2個のＤＣＴ係数は、秘密鍵Ｋに基づいて選択される。

【００８５】

図１４に戻り、ＳＮＲ計算部２８は、L_2種類の第２埋め込みホストデータの候補U^{k}に対して第２透かしデータy^{k}の耐性、すなわち埋め込み強度を評価し（Ｓ１６）、セレクタ３０は埋め込み強度が最大となる第２埋め込みホストデー

タの候補Ｕ^{k}を最終的な第２埋め込みホストデータＵとして選択する（Ｓ１８）。

【００８６】

埋め込み強度の評価式を与える前に、第２埋め込みホストデータＵに対して信号処理や画像処理などにより変形が加えられた場合に、第２透かしデータＹ＾がどのように検出されるかを検討する。第２埋め込みホストデータＵに加えられる変形をノイズＮとして扱い、ノイズＮが加わった埋め込みホストデータＵを第２埋め込みホスト信号Ｕ＾と呼ぶ。この第２埋め込みホスト信号Ｕ＾から第２透かしデータＹ＾を抽出する方法を説明する。第２埋め込みホスト信号の集合のペア（Ｕ＾$^{+}$，Ｕ＾$^{-}$）を次のように定義する。第２埋め込みホスト信号の集合Ｕ＾$^{+}$，Ｕ＾$^{-}$は次のようにそれぞれ（n_2+r_2）個の要素をもつ。

【００８７】

$$U\hat{}^{+}=\{u\hat{}^{+}_0,\ u\hat{}^{+}_1,\ \cdots,\ u\hat{}^{+}_{n2+r2-1}\}$$

$$U\hat{}^{-}=\{u\hat{}^{-}_0,\ u\hat{}^{-}_1,\ \cdots,\ u\hat{}^{-}_{n2+r2-1}\}$$

ここで第２埋め込みホスト信号の集合Ｕ＾$^{+}$，Ｕ＾$^{-}$の要素である各サブセット$u\hat{}^{+}_i$、$u\hat{}^{-}_i$は、電子透かしの埋め込み位置に対応して、次のように埋め込みホスト信号Ｕ＾のm_2個のサンプルデータからなる。

$$u\hat{}^{+}_i=\{u\hat{}^{+}_{i,0},\ u\hat{}^{+}_{i,1},\ \cdots,\ u\hat{}^{+}_{i,m2-1}\}$$

$$u\hat{}^{-}_i=\{u\hat{}^{-}_{i,0},\ u\hat{}^{-}_{i,1},\ \cdots,\ u\hat{}^{-}_{i,m2-1}\}$$

【００８８】

第２透かしビットy^{k}_iを検出するために、次の検出値z_iを計算する。

$$z_i=\Sigma_{j=0}^{m2-1}(u\hat{}^{+}_{i,j}-u\hat{}^{-}_{i,j})$$

$$=\Sigma_{j=0}^{m2-1}[(u^{+}_{i,j}+n^{+}_{i,j})-(u^{-}_{i,j}+n^{-}_{i,j})]$$

$$=\Sigma_{j=0}^{m2-1}[(\omega^{+}_{i,j}-\omega^{-}_{i,j})+(\beta^{+}_{i,j}+\beta^{-}_{i,j})\cdot y^{k}_i+(n^{+}_{i,j}-n^{-}_{i,j})]$$

ここで$\Sigma_{j=0}^{m2-1}(\omega^{+}_{i,j}-\omega^{-}_{i,j})$は$m_2$が十分に大きいとき、一般にガウス分布に従い、０に近づく。またノイズの項$\Sigma_{j=0}^{m2-1}(n^{+}_{i,j}-n^{-}_{i,j})$についても同様に０に近づく。したがって、$z_i$は$\Sigma_j$

$=0^{m2-1}[(\beta^{+}_{i,j}+\beta^{-}_{i,j})\cdot y^{k}_{i}]$の値で近似できる。（$\beta^{+}_{i,j}+\beta^{-}_{i,j}$）は正であるから、第２透かしビット$y^{k}_{i}$が１ならば$z_i$は正であり、第２透かしビッド$y^{k}_{i}$が－１ならば$z_i$は負である。したがって$z_i$の正負により第２透かしビット$y^{k}_{i}$の値を判定することができる。

【００８９】

埋め込み強度の評価は、第１埋め込みホストデータＷを第２透かしデータＹに対するノイズとみなして、埋め込まれた透かしデータＹに対して検出される透かしデータの分散を計算することにより行われる。分散が小さいほど、耐性が強いと考えることができる。第２埋め込みホストデータの候補のペア（U^{+k}，U^{-k}）に対して次式によりＳＮ比を評価して、最適な候補Ｋを選択する。

【００９０】

$$K=\mathrm{argmax}_{k}\,(P_k/\sigma_k^{2})$$

$$P_k=\Sigma_{i=0}^{n2+r2-1}\left|\Sigma_{j=0}^{m2-1}(u^{+k}_{i,j}-u^{-k}_{i,j})\right|^{2}/(n_2+r_2)$$

$$\sigma_k^{2}=\Sigma_{i=0}^{n2+r2-1}\left|\Sigma_{j=0}^{m2-1}(u^{+k}_{i,j}-u^{-k}_{i,j})-P_k^{1/2}\cdot y^{k}_{i}\right|^{2}/(n_2+r_2)$$

【００９１】

第２透かしビットy^{k}_{i}が｛１，－１｝のいずれであるかを判定するための前述の検出値z_iは、第２埋め込みホストデータＵにノイズが付加される前の状態では、$z_i=\Sigma_{j=0}^{m2-1}(u^{+k}_{i,j}-u^{-k}_{i,j})$で与えられることを考慮すると、分散$\sigma_k^{2}$は、第２透かしビットに関する検出値$z_i$と実際に埋め込まれた第２透かしビットの平均値$P_k^{1/2}\cdot y^{k}_{i}$との差の自乗をｉ＝０，・・・，$n_2+r_2-1$について評価して平均化したものであると言える。ただし、P_kは検出値z_iのｉ＝０，・・・，n_2+r_2-1についての自乗平均であり、埋め込まれた透かしの平均パワーを示す。したがって、埋め込まれた第２透かしデータy^{k}と抽出される透かしデータとの間のユークリッド距離が小さく、第２透かしビットを抽出するための検出値の絶対値が大きいほど、P_k/σ_k^{2}の値は大きくなる。言い換えれば、P_k/σ_k^{2}が最大となる候補を選択することは、第２透かしビットの検出誤差が最小である候補を選択することを意

味する。

【００９２】

検出値z_iについて、$\omega^+_{i,j} > \omega^-_{i,j}$かつ$y^k_i = 1$ならば$z_i >> 0$となり、$\omega^+_{i,j} < \omega^-_{i,j}$かつ$y^k_i = -1$ならば$z_i << 0$となる。したがって前述の評価により最適な第２透かしデータy^kの候補を選択することは、検出値z_iによる第２透かしビットy^k_iの検出性能を向上させるために、$\omega^+_{i,j} > \omega^-_{i,j}$ならば$y'_i = 1$となり、$\omega^+_{i,j} < \omega^-_{i,j}$ならば$y'_i = -1$となるように、元の透かしビット$y_i$を$y'_i$に変更することを意味する。これがＧＳ方式のガイディングルールであり、これにより検出値z_iのレスポンスが改善する。

【００９３】

（３）第２透かしＹの抽出手順

第２透かし抽出ブロック２１０の第２抽出部４０は、ノイズの付加された第２埋め込みホスト信号Ｕ＾を受け取ると、ＥＣＣ復号部４４が硬入力の復号器で構成される場合には、検出値z_iを次式に示すように計算し、検出値z_iの正負で、第２透かしビット$y^_i$が｛－１，１｝のいずれであるかを判定し、第２透かしデータＹ＾を得る。また、ＥＣＣ復号部４４が軟入力の復号器で構成される場合には、検出値z_iを｛－１，１｝に硬判定することなく、そのまま、ＥＣＣ復号部４４に送る。

【００９４】

$$z_i = \Sigma_{j=0}^{m2-1} (u^{\wedge +}_{i,j} - u^{\wedge -}_{i,j})$$
$$= \Sigma_{j=0}^{m2-1} [(u^+_{i,j} + n^+_{i,j}) - (u^-_{i,j} + n^-_{i,j})]$$
$$\fallingdotseq \Sigma_{j=0}^{m2-1} [(\omega^+_{i,j} - \omega^-_{i,j}) + (\beta^+_{i,j} + \beta^-_{i,j}) \cdot y_i]$$

【００９５】

抽出された第２透かしデータＹ＾はさらにＥＣＣ復号部４４により誤り訂正がなされ、デスクランブラ４６によりスクランブルを解除されて出力される。

【００９６】

（４）第２透かしの除去手順

第２透かし抽出ブロック２１０の第２透かし除去部４２による第２透かしの除去手順を説明する。第２埋め込みホスト信号Ｕ＾から検出された第２透かしデータＹ＾による変化分を次のように除去して第１埋め込みホスト信号Ｗ＾を取得する。

$$\omega\hat{}^{+}_{i,j}=u\hat{}^{+}_{i,j}-\beta\hat{}^{+}_{i,j}\cdot y\hat{}_{i}$$
$$=\omega^{+}_{i,j}+(\beta^{+}_{i,j}\cdot y_{i}-\beta\hat{}^{+}_{i,j}\cdot y\hat{}_{i})+n^{+}_{i}$$
$$=\omega^{+}_{i,j}+q^{+}_{i,j}+n^{+}_{i}$$
$$\omega\hat{}^{-}_{i,j}=u\hat{}^{-}_{i,j}+\beta\hat{}^{-}_{i,j}\cdot y\hat{}_{i}$$
$$=\omega^{-}_{i,j}-(\beta^{-}_{i,j}\cdot y_{i}-\beta\hat{}^{-}_{i,j}\cdot y\hat{}_{i})+n^{-}_{i}$$
$$=\omega^{-}_{i,j}-q^{-}_{i,j}+n^{-}_{i}$$

ここで、$\beta\hat{}^{+}_{i,j}$および$\beta\hat{}^{-}_{i,j}$は上述の人間の視覚モデルによるスケーリングパラメータ$\beta^{+}_{i,j}$および$\beta^{-}_{i,j}$の近似値である。第２透かしに関するスケーリングパラメータが、視覚モデルではなく、秘密鍵に基づいて計算されるデータの場合には、第２透かしの埋め込み時、抽出時共に同一の値を発生させることができるため、$\beta^{+}_{i,j}=\beta\hat{}^{+}_{i,j}$，$\beta^{-}_{i,j}=\beta\hat{}^{-}_{i,j}$となり、さらに、第２透かしビット$y\hat{}_{i}$が正しく検出される場合、すなわち、$y\hat{}_{i}=y_{i}$の場合、$q^{\pm}_{i,j}=0$となり、第２透かしを完全に除去することが可能である。視覚モデルを用いた場合には、埋め込み時と抽出時においては、スケーリングパラメータを計算する対象の画像は異なるものの、両画像の違いを認知できないほど似通っているため、$\beta^{+}_{i,j}\fallingdotseq\beta\hat{}^{+}_{i,j}$，$\beta^{-}_{i,j}\fallingdotseq\beta\hat{}^{-}_{i,j}$となる。以上により、第２透かしビット$y\hat{}_{i}$が正しく検出される場合、すなわち、$y_{i}=y\hat{}_{i}$の場合、第２透かしの除去により発生したノイズ$q^{\pm}_{i,j}$はゼロに近似される。

【００９７】

（５）第１透かしの抽出手順

第１透かし抽出ブロック２２０の第１抽出部４８による第１透かしの抽出手順を説明する。第１抽出部４８は、第２透かし抽出ブロック２１０から第２透かしＹ＾が除去された第１埋め込みホスト信号Ｗ＾を受け取り、第１透かしビットｘ

$_i$を検出するために、次の検出値z_iを計算する。

$$z_i=\Sigma_{j=0}^{m1-1}(w\hat{}+_{i,j}-w\hat{}-_{i,j})$$
$$=\Sigma_{j=0}^{m1-1}[(v+_{i,j}-v-_{i,j})+(\alpha+_{i,j}+\alpha-_{i,j})\cdot x_i+(q\sim+_{i,j}+q\sim-_{i,j})+(n\sim+_{i,j}-n\sim-_{i,j})]$$

ただし、$q\sim\pm_{i,j}$は、元のホストデータ$v\pm_{i,j}$に埋め込まれている第２透かしビットの除去後に生じたノイズである。また、$n\sim\pm_{i,j}$は、信号処理などにより、元のホストデータ$v\pm_{i,j}$に加えられたノイズを示す。

【００９８】

ここで$\Sigma_{j=0}^{m1-1}(v+_{i,j}-v-_{i,j})$は$m_1$が十分に大きいとき、一般にガウス分布に従い、０に近づく。ノイズの項$\Sigma_{j=0}^{m1-1}(n+_{i,j}-n-_{i,j})$についても同様に０に近づく。$\Sigma_{j=0}^{m1-1}(q\sim+_{i,j}+q\sim-_{i,j})$の項についても、第２透かしが正しく抽出されている場合には、０に近似できる。したがって、検出値z_iは$\Sigma_{j=0}^{m-1}[(\alpha+_{i,j}+\alpha-_{i,j})\cdot x_i]$の値で近似できる。$(\alpha+_{i,j}+\alpha-_{i,j})$は正であるから、第１透かしビット$x_i$が１ならば$z_i$は正であり、第１透かしビット$x_i$が－１ならば$z_i$は負である。したがって$z_i$の正負により第１透かしビット$x_i$の値を判定することができる。

【００９９】

以上のことより、検出値z_iは、次式のように近似される。

$$z_i=\Sigma_{j=0}^{m1-1}(w\hat{}+_{i,j}-w\hat{}-_{i,j})$$
$$\fallingdotseq\Sigma_{j=0}^{m1-1}[(v+_{i,j}-v-_{i,j})+(\alpha+_{i,j}+\alpha-_{i,j})\cdot x_i]$$

【０１００】

第１透かし抽出ブロック２２０の第１抽出部４８は、第１埋め込みホスト信号$W\hat{}$を受け取り、検出値z_iを計算した後、ＥＣＣ復号部４５が硬入力の復号器で構成される場合には、検出値z_iの正負で、第１透かしビット$x_i\hat{}$が｛－１，１｝のいずれであるかを判定し、第１透かしデータ$X\hat{}$を得る。また、ＥＣＣ復号部４５が軟入力の復号器で構成される場合には、検出値z_iを｛－１，１｝

に硬判定することなく、そのまま、ＥＣＣ復号部４５に送る。

【０１０１】

抽出された第１透かしデータＸ＾はさらにＥＣＣ復号部４５により誤り訂正がなされて出力される。

【０１０２】

（６）透かしベクトルの許容劣化領域

図１５は、ＧＳ方式によるホストデータＶに対する透かしビット系列の候補を説明する図である。透かし埋め込み対象のホストデータｖをホストデータの信号空間のある１点であるとすると、このホストデータｖに対して人間の視覚モデルから決定される知覚上の劣化を生じない非線形領域（以下許容劣化領域３００という）が同図のように定まる。ただし、説明の便宜上、信号空間を２次元空間で示している。透かし系列の候補数が１６の場合、第１透かしベクトルの候補x_0～x_{15}がスクランブルにより得られる。これらの第１透かしベクトル候補x_i（ｉ＝０，・・・，１５）をホストデータｖに加算する際、許容劣化領域３００に収まるようにスケーリングパラメータα_iを乗算することで透かしの増幅を行う。その結果、１６個の第１埋め込みホストデータの候補w_0，・・・，w_{15}が得られる。これらの候補の中で埋め込み透かしのＳＮ比が最大のものを選択すると、同図の例では、ベクトル長が最大である第１埋め込みホストデータw_5が得られる。

【０１０３】

次に、第２透かしベクトルの候補y_i（ｉ＝０，・・・，１５）をスクランブルにより生成して、最適な第１埋め込みホストデータw_5に同様に埋め込むと、図１６に示すように、最適な第１埋め込みホストデータw_5に対して決定される許容劣化領域３１０内で、１６個の第２埋め込みホストデータの候補u_0，・・・，u_{15}が得られる。これらの候補の中で埋め込み透かしのＳＮ比が最大のものを選択すると、同図のように最適な第２埋め込みホストデータu_9が得られる。

【０１０４】

ここで、最適な第２埋め込みホストデータu_9は元のホストデータｖの許容劣

化領域３００内には収まっていない。このように透かしを多重に埋め込むと、一般には多重埋め込みホストデータは、元のホストデータの許容劣化領域内に収まらないことになる。そこで、図１７に示すように、ホストデータｖの許容劣化領域３００と第１透かし埋め込み後の最適な第１埋め込みホストデータw_5に対して決定される許容劣化領域３１０との共通領域３１２内に制限して、第２埋め込みホストデータの候補を選択する。共通領域３１２内で埋め込み透かしのＳＮ比が最大のものを選択すると、同図のように、最適な第２埋め込みホストデータu_{11}が得られ、二重埋め込みホストデータは元のホストデータｖの許容劣化領域３００内に収まる。多重に透かしを埋め込む場合も同様の制限を行い、多重埋め込みホストデータが元のホストデータｖの許容劣化領域３００内に収まるようにすることができる。

【０１０５】

第２埋め込みホストデータの選択範囲を広げるために、図１８のように、緩和係数Ａ（＞１）により、スケーリングパラメータαを$\alpha \cdot A$に緩和して、ホストデータｖの許容劣化領域３００を緩和許容劣化領域３０２に広げてもよい。この場合、ホストデータｖの緩和許容劣化領域３０２と最適な第１埋め込みホストデータw_5に対して決定される許容劣化領域３１０との共通領域３１４内に制限して、第２埋め込みホストデータの候補を選択するため、選択対象の候補が増え、ベクトル長がより長いu_{10}が最適な第２埋め込みホストデータとして得られる。

【０１０６】

以下、図１７および図１８の第２埋め込みホストデータの候補U^kの選択手順を詳細に述べる。ＧＳ方式により第１透かしの埋め込みを行った場合、第１埋め込みホストデータＷは次式で与えられる。

$$w^+_{i,j} = v^+_{i,j} + \alpha^+_{i,j} \cdot x^k_i$$

$$w^-_{i,j} = v^-_{i,j} - \alpha^-_{i,j} \cdot x^k_i$$

ただし、$\{v^{\pm}_{i,j}\}$（$i=0,\cdots,n_1-1$，$j=0,\cdots,m_1-1$）はホストデータＶから秘密鍵K_1にもとづいて選択されたサンプル集合である。

【０１０７】

第２埋め込みホストデータの候補Ｕ^{k}は次式で与えられる。

$u^{k+}_{i,j}=w^{\sim+}_{i,j}+\beta^{+}_{i,j}\cdot y^{k}_{i}$

$u^{k-}_{i,j}=w^{\sim-}_{i,j}-\beta^{-}_{i,j}\cdot y^{k}_{i}$

ただし、$\{w^{\sim\pm}_{i,j}\}$（$i=0,\cdots,n_2-1$，$j=0,\cdots,m_2-1$）は第１埋め込みホストデータＷから秘密鍵Ｋ$_2$にもとづいて選択されたサンプル集合である。このサンプル集合 $\{w^{\sim\pm}_{i,j}\}$ は、第１透かしデータＸの埋め込み対象として秘密鍵Ｋ$_1$にもとづいて選択されたサンプル集合 $\{v^{\pm}_{i,j}\}$ とは異なる集合であり、サンプル集合 $\{v^{\pm}_{i,j}\}$ とは独立に選択される。したがって、第１透かしデータＸの埋め込み式における$w^{\pm}_{i,j}$とは区別して$w^{\sim\pm}_{i,j}$と表記している。

【０１０８】

ここで、$w^{\sim\pm}_{i,j}$は元のホストデータの値$v^{\sim\pm}_{i,j}$から$\Delta^{\pm}_{i,j}$だけ変化していることから、

$u^{k+}_{i,j}=v^{\sim+}_{i,j}+\Delta^{+}_{i,j}+\beta^{+}_{i,j}\cdot y^{k}_{i}$

$u^{k-}_{i,j}=v^{\sim-}_{i,j}+\Delta^{-}_{i,j}-\beta^{-}_{i,j}\cdot y^{k}_{i}$

と表すことができる。ここで$\Delta^{\pm}_{i,j}$の値は、埋め込まれている第１透かしビットの値により、$+\alpha^{\sim\pm}_{i,j}$または$-\alpha^{\sim\pm}_{i,j}$である。もしくは、第１透かしビットがサンプル$v^{\sim\pm}_{i,j}$に埋め込まれていない場合は、$\Delta^{\pm}_{i,j}=0$となる。なお、$v^{\sim\pm}_{i,j}$は秘密鍵Ｋ$_2$により決定されたサンプル$w^{\sim\pm}_{i,j}$と同じ場所に位置する原ホストデータＶのサンプルであり、$\alpha^{\sim\pm}_{i,j}$は、その原サンプル$v^{\sim\pm}_{i,j}$において決定されたスケーリングパラメータである。

【０１０９】

（$\Delta^{\pm}_{i,j}\pm\beta^{\pm}_{i,j}\cdot y^{k}_{i}$）の値は、透かしを二重に埋め込んだことによる原サンプル$v^{\sim\pm}_{i,j}$からの変化量である。一方、$\alpha^{\sim\pm}_{i,j}$は、その原サンプル$v^{\sim\pm}_{i,j}$に対して許容される最大の変化量である。したがって、添え字の集合Ｃを次のように定義し、ｋ∈Ｃとなる候補について、ＳＮ比が最大になるものを選択すればよいことがわかる。

$$K=\mathrm{argmax}_{k\in C}(P_k/\sigma_k^2)$$

$$P_k=\Sigma_{i=0}^{n2-1}|\Sigma_{j=0}^{m2-1}(u^+k_{i,j}-u^-k_{i,j})|^2/n_2$$

$$\sigma_k^2=\Sigma_{i=0}^{n2-1}|\Sigma_{j=0}^{m2-1}(u^+k_{i,j}-u^-k_{i,j})-P_k^{1/2}\cdot y^k{}_i|^2/n_2$$

$$C=\{c:|\Delta^+_{i,j}+\beta^+_{i,j}\cdot y^c{}_i|\leqq\alpha\sim^+_{i,j},\ |\Delta^-_{i,j}-\beta^-_{i,j}\cdot y^c{}_i|\leqq\alpha\sim^-_{i,j},\ \forall i=0,\cdots,n_2-1,\ \forall j=0,\cdots,m_2-1\}$$

【０１１０】

添え字の集合Ｃは、第２埋め込みホストデータの候補U^kのサンプル集合がすべてホストデータＶの許容劣化範囲に収まる領域を示しており、この領域内に存在するホストデータU^kの中からＳＮ比が最大のものが選択される。緩和許容劣化領域に広げる場合は、$\alpha\sim^+_{i,j}$，$\alpha\sim^-_{i,j}$をそれぞれ$A\cdot\alpha\sim^+_{i,j}$，$A\cdot\alpha\sim^-_{i,j}$に置き換えればよい。緩和係数Ａの導入により、透かしの耐性を強化できるが、ホストデータＶからの劣化は大きくなる。以上の手順を繰り返し適用すれば、ホストデータＶを劣化させることなく、複数の透かしを多重に埋め込むことができる。

【０１１１】

実施の形態４

図１９は実施の形態４に係る電子透かし埋め込み装置１００の構成を示す。本実施の形態では、透かし情報Ｉに非重要データと重要データが含まれ、電子透かし埋め込み装置１００は、非重要データを第１透かしデータＸとして、重要データを第２透かしデータＹとしてホストデータＶに埋め込む。重要データとは、たとえばコンテンツの識別データなどの保護情報であり、非重要データとは、そのコンテンツに関連するＵＲＬ（Uniform Resource Locator）などの予備情報である。

【０１１２】

暗号化部１０は、秘密鍵Ｋを用いて、透かし情報Ｉに含まれる非重要データと

重要データをそれぞれ第１透かしデータＸと第２透かしデータＹに暗号化して、それぞれ第１透かし埋め込みブロック１１０の変更部１３と第２透かし埋め込みブロック１２０の変更部１６に入力する。

【０１１３】

第１透かし埋め込みブロック１１０の変更部１３は、第１透かしデータＸをスクランブルして出力し、第１透かし埋め込み部１４は、秘密鍵Ｋを用いて、スクランブルされた第１透かしデータＸ’をホストデータＶに埋め込み、第１埋め込みホストデータＷを出力する。

【０１１４】

第２透かし埋め込みブロック１２０の変更部１６は、第２透かしデータＹをスクランブルして出力し、第２透かし埋め込み部１８は、秘密鍵Ｋを用いて、スクランブルされた第２透かしデータＹ’を第１埋め込みホストデータＷに埋め込み、第２埋め込みホストデータＵを出力する。

【０１１５】

一般に、電子透かしの耐性は透かしのデータ量とトレードオフの関係にある。非重要データが暗号化された第１透かしデータＸは、データ量を多くする代わりに、弱い耐性でホストデータＶに埋め込み、重要データが暗号化された第２透かしデータＹは、データ量を少なく抑え、埋め込みの際の冗長度を増加させることで強い耐性をもたせて第１埋め込みホストデータＷに埋め込む。

【０１１６】

第１透かし埋め込みブロック１１０の変更部１３と第１透かし埋め込み部１４は協同して、複数のスクランブルされた透かしデータＸ’を生成し、それぞれをホストデータＶに埋め込み、複数の第１埋め込みホストデータＷの候補を生成し、それらの候補の一つを選択する機能をもつ。

【０１１７】

図２０は、第１透かし埋め込みブロック１１０の変更部１３および第１透かし埋め込み部１４の機能構成図である。この構成は、図７の構成において、マルチプレクサ２０に入力される埋め込み位置情報Ｐ＊を第１透かしデータＸに置き換え、第１埋め込みホストデータＷに対する埋め込み処理を行う第２埋め込み部２

７をホストデータＶに対する埋め込み処理を行う第１埋め込み部２６に置き換えたものである。

【０１１８】

この図２０の構成は、第２透かし埋め込みブロック１２０の変更部１６および第２透かし埋め込み部１８の機能構成としても用いることができる。その場合、図２０において、マルチプレクサ２０に入力される第１透かしデータＸを第２透かしデータＹに置き換え、ホストデータＶに対する埋め込み処理を行う第１埋め込み部２６を第１埋め込みホストデータＷに対する埋め込み処理を行う第２埋め込み部２７に置き換えればよい。もっともこの場合、図２０の構成を第２透かし埋め込みブロック１２０で流用することも可能である。すなわち、セレクタ３０が出力する第１埋め込みホストデータＷを第１埋め込み部２６にフィードバックして入力として与え、マルチプレクサ２０に第２透かしデータＹを入力すれば、第２透かし埋め込みブロック１２０の動作をなすことができる。このように構成することにより、第１透かし埋め込みブロック１１０と第２透かし埋め込みブロック１２０の機能を実質的に同一の構成で実現して、ハードウエアまたはソフトウエアの構成を簡略にすることができる。

【０１１９】

図２１は、実施の形態４に係る電子透かし抽出装置２００の構成を示す。図２１の第２透かし抽出ブロック２１０の構成と動作は、図８の第２透かし抽出ブロック２１０と同様であるが、デスクランブラ４６が出力する第２透かしデータＹは、第１透かし抽出ブロック２２０の第１抽出部４８には供給されずに、そのまま電子透かし抽出装置２００から出力される。

【０１２０】

図２１の第１透かし抽出ブロック２２０の第１抽出部４８とＥＣＣ復号部４５は、それぞれ図８の第１透かし抽出ブロック２２０の第１抽出部４８とＥＣＣ復号部４５と同様の動作を行うが、図２１の第１透かし抽出ブロック２２０の第１抽出部４８は第１透かしデータの埋め込み位置情報を利用しない点が異なる。また、図２１の第１透かし抽出ブロック２２０では、ＥＣＣ復号部４５の出力する第１透かしデータＸ＾$_b$のスクランブルを解除し、先頭部の初期データを取り除

いて第１透かしデータＸ＾を出力する。

【０１２１】

第１透かし抽出ブロック２２０の第１抽出部４８、ＥＣＣ復号部４５、およびデスクランブラ４７の機能は、第２透かし抽出ブロック２１０の第２抽出部４０、ＥＣＣ復号部４４、およびデスクランブラ４６を流用して実現することもできる。すなわち、第２透かし除去部４２から出力される第２透かしが除去された第１埋め込みホスト信号Ｗ＾をフィードバックして第２抽出部４０の入力として与えれば、第１透かし抽出ブロック２２０の機能を実現することができ、構成を簡略化することができる。

【０１２２】

第１透かしデータＸは第２透かしデータＹに比べて、データ量が多く、耐性が弱いため、第２埋め込みホストデータＵに比較的弱いノイズが加えられた場合は、第１透かしデータＸと第２透かしデータＹがともに正しく検出されるが、強いノイズが加えられた場合は、耐性の弱い第１透かしデータＸは壊れる。しかし、耐性の強い第２透かしデータＹは正しく検出されるので、重要データをノイズが強い場合でも検出することができるようになる。

【０１２３】

また、先に埋め込まれる第１透かしデータＸの方が第２透かしデータＹよりも強い耐性をもつようにしてもよい。ただし、第１透かしデータＸは、可逆埋め込み方式により埋め込まれるものとする。すなわち、埋め込みの順序を逆にして、先に重要データを含む第１透かしデータＸを強い耐性で埋め込み、非重要データをその後に埋め込むことも可能である。この場合、抽出側では、最初に耐性の強い重要データに関する第１透かしデータＸを抽出して、抽出したビットを用いて埋め込みの逆演算を行い、第２透かしデータＹとの干渉を除去する。その後、第２透かしデータＹを抽出する。第１透かしデータＸと第２透かしデータＹは互いに干渉しないため、必ずしも埋め込まれた順序と逆の順に透かしを抽出する必要はない。

【０１２４】

以上述べたように、実施の形態によれば、電子透かしを埋め込む対象となるメ

ディアデータが与えられると、そのメディアデータに応じて、透かしデータを埋め込み易い位置を検出して、透かしを埋め込むことができ、埋め込まれる透かしの耐性を強化することができる。また、ＧＳ方式を用いて、透かしビット系列をそのメディアデータに埋め込みやすいビット系列に変換した上で埋め込むことができる。したがって信号処理、幾何変換、圧縮、データの改ざんなどに対する電子透かしの耐性を強化することができ、透かしの検出精度が大幅に改善する。

【０１２５】

また、透かしが多重に埋め込まれたメディアデータに対して、透かしを順次抽出する際、先に抽出した透かしデータをメディアデータから完全に除去した後に、次の透かしデータを抽出するため、複数の透かしの干渉による誤検出を防ぐことができる。

【０１２６】

以上、本発明を実施の形態をもとに説明した。これらの実施の形態は例示であり、それらの各構成要素や各処理プロセスの組み合わせにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【０１２７】

そのような変形例として、実施の形態１の実透かし埋め込み部１１２およびメタ透かし埋め込み部１２２に、それぞれ実施の形態４の第１透かし埋め込みブロック１１０および第２透かし埋め込みブロック１２０の機能構成を利用して、ＧＳ方式で実透かしとメタ透かしの埋め込みを行うようにしてもよい。また実施の形態２の実透かし埋め込み部１１２および第２透かし埋め込み部１２４に、それぞれ実施の形態３の第１透かし埋め込みブロック１１０および第２透かし埋め込みブロック１２０の機能構成を利用して、埋め込み位置情報をＧＳ方式でスクランブルするようにしてもよい。

【０１２８】

複数の透かしデータの候補を生成するために、多様性に富んだ候補の生成が可能なＧＳ方式を用いたが、他のスクランブル方式を適用してもよく、また何らかの方法でランダムに候補のデータを生成してもよい。また実施の形態では、逆ス

クランブルにより、抽出された透かしデータから元の透かしデータを再現したが、複数種類のスクランブルされた透かしデータと元の透かしデータとを対応づけたテーブルを備え、このテーブルを参照して元の透かしデータを求めてもよい。

【０１２９】

またスクランブルの際に初期データとして使用した識別データは、透かしデータの先頭に挿入されて復号側に提供されていたが、この識別データを透かしには埋め込まずに、符号化側で秘密鍵として保持、管理してもよい。その場合、復号側はこの秘密鍵を取得した上で、透かしデータのスクランブルを解除する。あるいは、識別データを新たな透かしデータとして、ホストデータに埋め込んでもよい。

【０１３０】

上記のいずれの実施の形態においても、第１透かしの埋め込み後に第２透かしを埋め込む構成を説明したが、埋め込み順序を逆にして、第１透かしを埋め込む前に第２透かしを埋め込み、第２透かし埋め込み後のホストデータに第１透かしを埋め込んでもよい。第１透かしの埋め込み位置情報を第２透かしとして埋め込む場合であっても、第１透かしの埋め込み位置を先に決定し、第１透かしは埋め込まずにいったんメモリに記憶しておく。そして、第１透かしの埋め込み位置情報を第２透かしとして先にホストデータに埋め込み、その後メモリから第１透かしのデータを読み出して、第１透かしをホストデータに埋め込む。この場合、第２透かし埋め込みブロック１２０による第２透かし埋め込み後のホストデータの出力が第１透かし埋め込みブロック１１０に埋め込み対象のホストデータとして入力される構成にすればよい。

【発明の効果】

本発明によれば、電子透かしの耐性が向上し、透かしの検出精度が改善する。

【図面の簡単な説明】

【図１】　実施の形態１に係る電子透かし埋め込み装置の構成図である。

【図２】　実施の形態１に係る電子透かし抽出装置の構成図である。

【図３】　実施の形態２に係る電子透かし埋め込み装置の構成図である。

【図４】　実施の形態２に係る電子透かし抽出装置の構成図である。

【図５】　実施の形態３に係る電子透かし埋め込み装置の構成図である。

【図６】　図５の第１透かし埋め込みブロックの機能構成図である。

【図７】　図５の第２透かし埋め込みブロックの機能構成図である。

【図８】　実施の形態３に係る電子透かし抽出装置の構成図である。

【図９】　図６の第１透かし埋め込みブロックによる第１透かしデータの埋め込み手順を説明するフローチャートである。

【図１０】　第２透かしデータとスクランブルされた第２透かしデータとの関係を説明する図である。

【図１１】　透かし埋め込み時の畳み込み演算を説明する図である。

【図１２】　透かし抽出時の畳み込み演算を説明する図である。

【図１３】　図１３（ａ）、（ｂ）は、スクランブルされた透かしデータの埋め込み方法を説明する図である。

【図１４】　図７の第２透かし埋め込みブロックによる第２透かしデータの埋め込み手順を説明するフローチャートである。

【図１５】　第１透かしベクトルの候補の空間を説明する概念図である。

【図１６】　第２透かしベクトルの候補の空間を説明する概念図である。

【図１７】　第２透かしベクトルの最適な選択例を説明する図である。

【図１８】　第２透かしベクトルの別の最適な選択例を説明する図である。

【図１９】　実施の形態４に係る電子透かし埋め込み装置の構成図である。

【図２０】　図１９の第１透かし埋め込みブロックの機能構成図である。

【図２１】　実施の形態４に係る電子透かし抽出装置の構成図である。

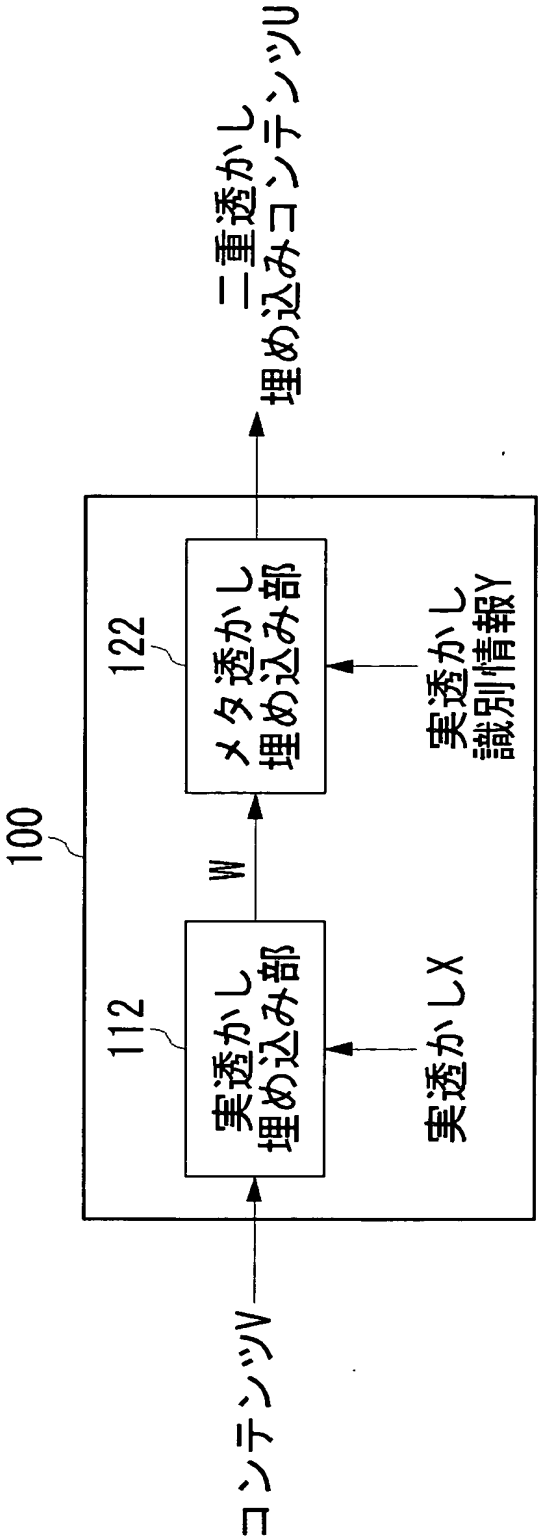
【符号の説明】

１０　暗号化部、　１２　位置検出部、　１４　第１透かし埋め込み部、　１６　変更部、　１８　第２透かし埋め込み部、　２０　マルチプレクサ、　２２　スクランブラ、　２４　ＥＣＣ部、　２６　第１埋め込み部、　２７　第２埋め込み部、　２８　ＳＮＲ計算部、　３０　セレクタ、　４０　第２抽出部、　４２　第２透かし除去部、　４４　ＥＣＣ復号部、　４６　デスクランブラ、　４８　第１抽出部、　６０　位置情報生成部、　１００　電子透かし埋め込み装置、　１１０　第１透かし埋め込みブロック、　１２０　第２透かし埋め込みブ

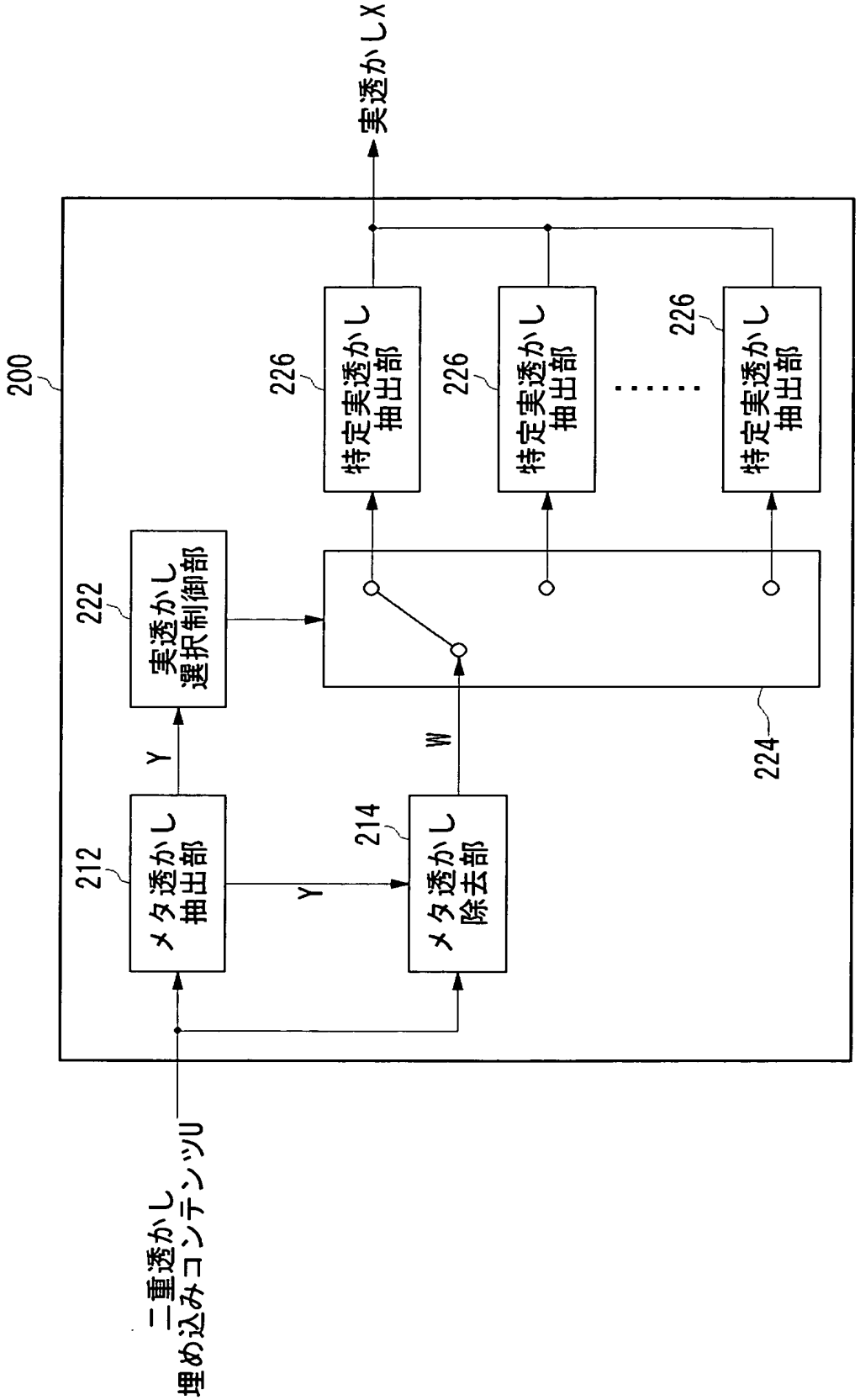
ロック、　２００　電子透かし抽出装置、　２１０　第２透かし抽出ブロック、
２２０　第１透かし抽出ブロック。

【書類名】　図面

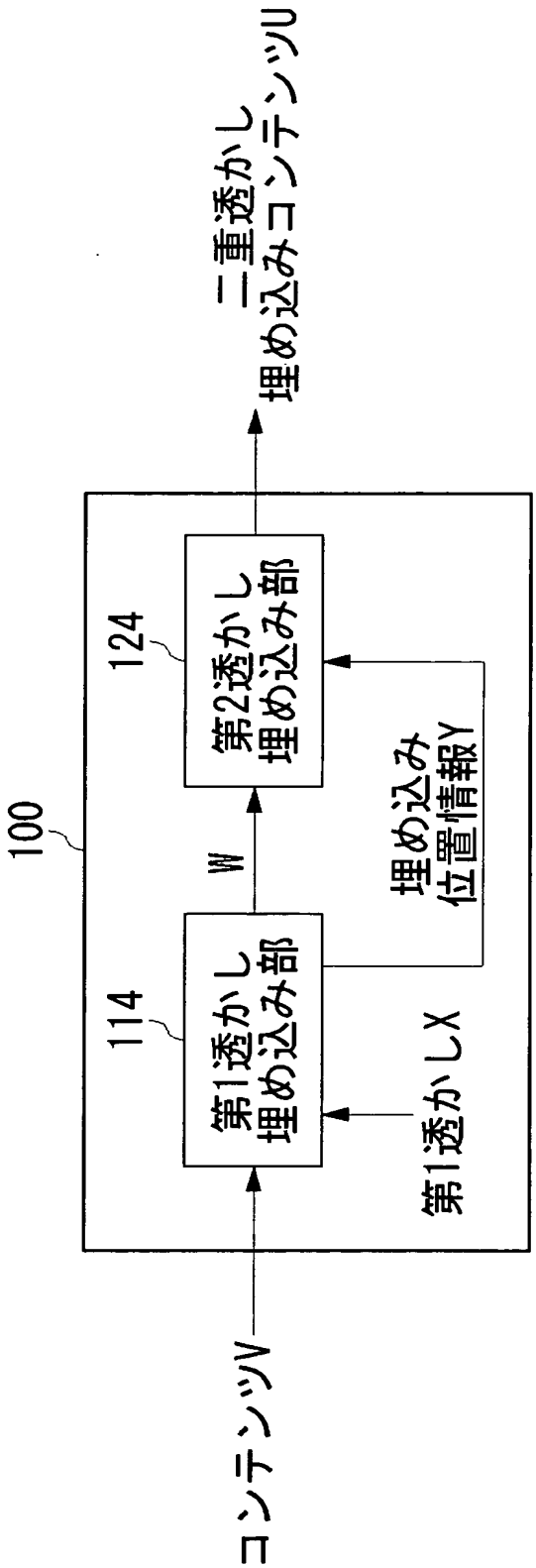
【図１】


二重透かし
埋め込みコンテンツU
100
122
メタ透かし
埋め込み部
実透かし
識別情報Y
W
112
実透かし
埋め込み部
実透かしX
コンテンツV

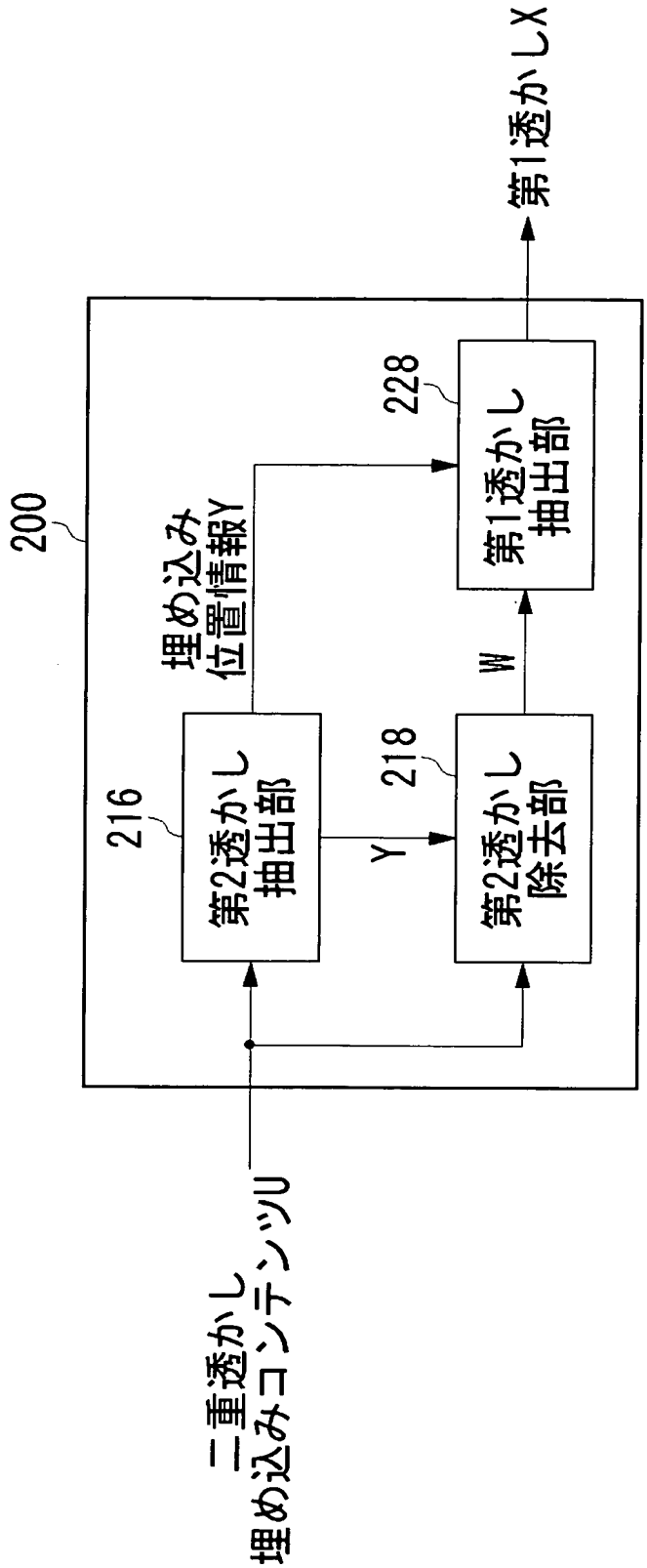
【図２】


実透かしX
200
226
特定実透かし抽出部
226
特定実透かし抽出部
226
特定実透かし抽出部
222
実透かし選択制御部
224
212
メタ透かし抽出部
214
メタ透かし除去部
Y
Y
W
二重透かし埋め込みコンテンツU

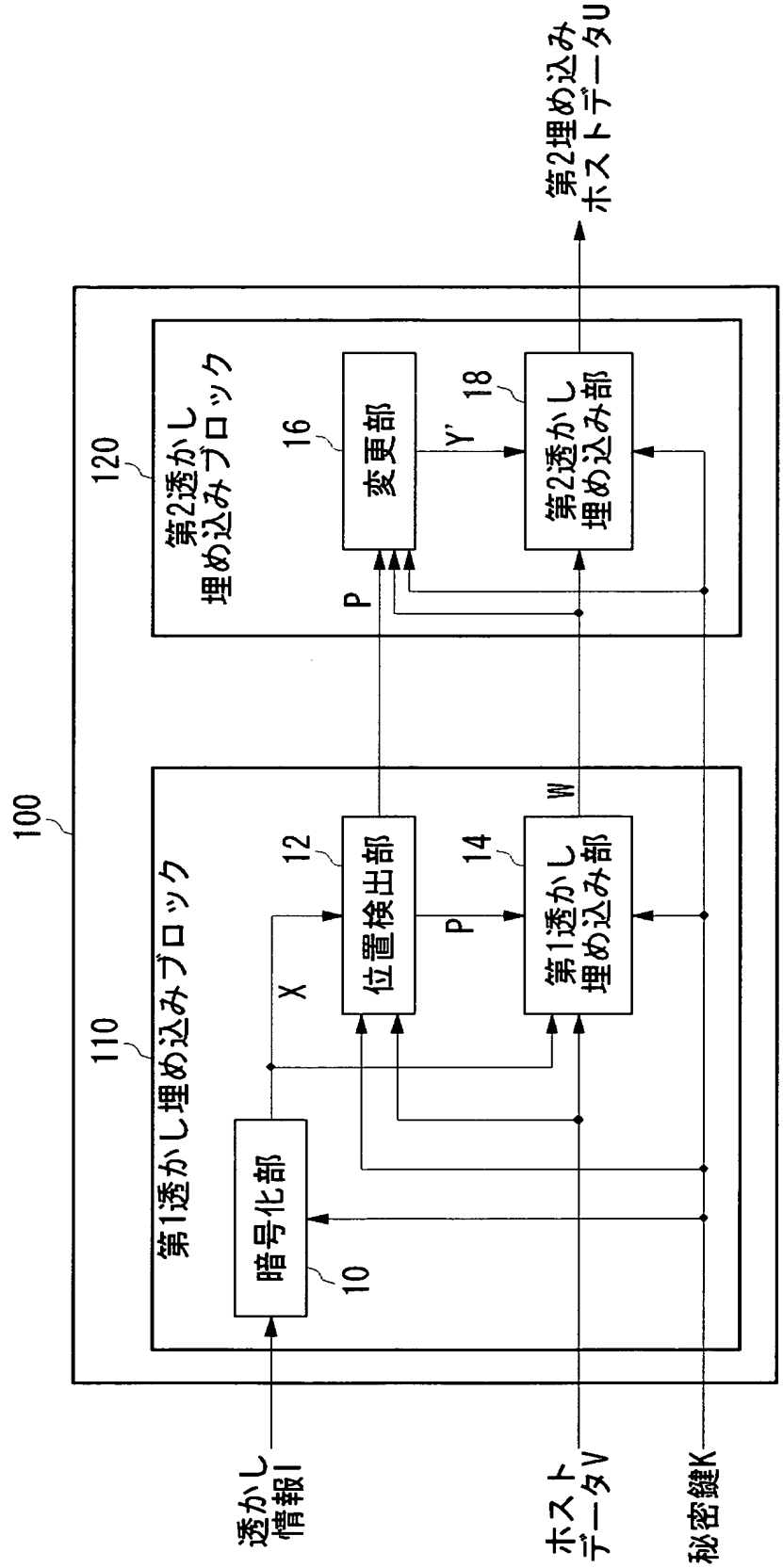
【図３】


二重透かし
埋め込みコンテンツU
124
第2透かし
埋め込み部
100
W
埋め込み
位置情報Y
114
第1透かし
埋め込み部
第1透かしX
コンテンツV

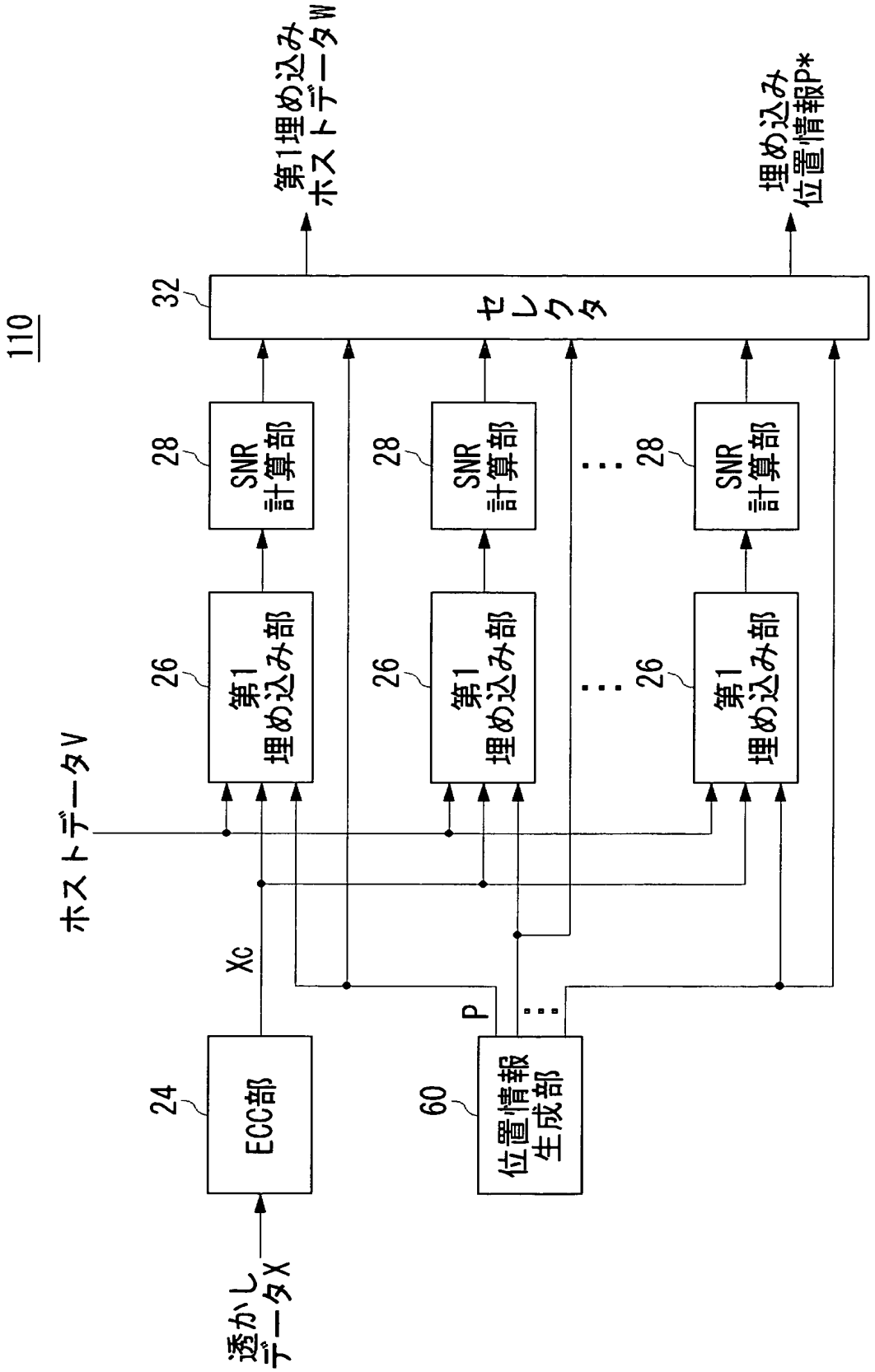
【図４】


二重透かし
埋め込みコンテンツU
200
216
第2透かし
抽出部
埋め込み
位置情報Y
Y
218
第2透かし
除去部
W
228
第1透かし
抽出部
第1透かしX

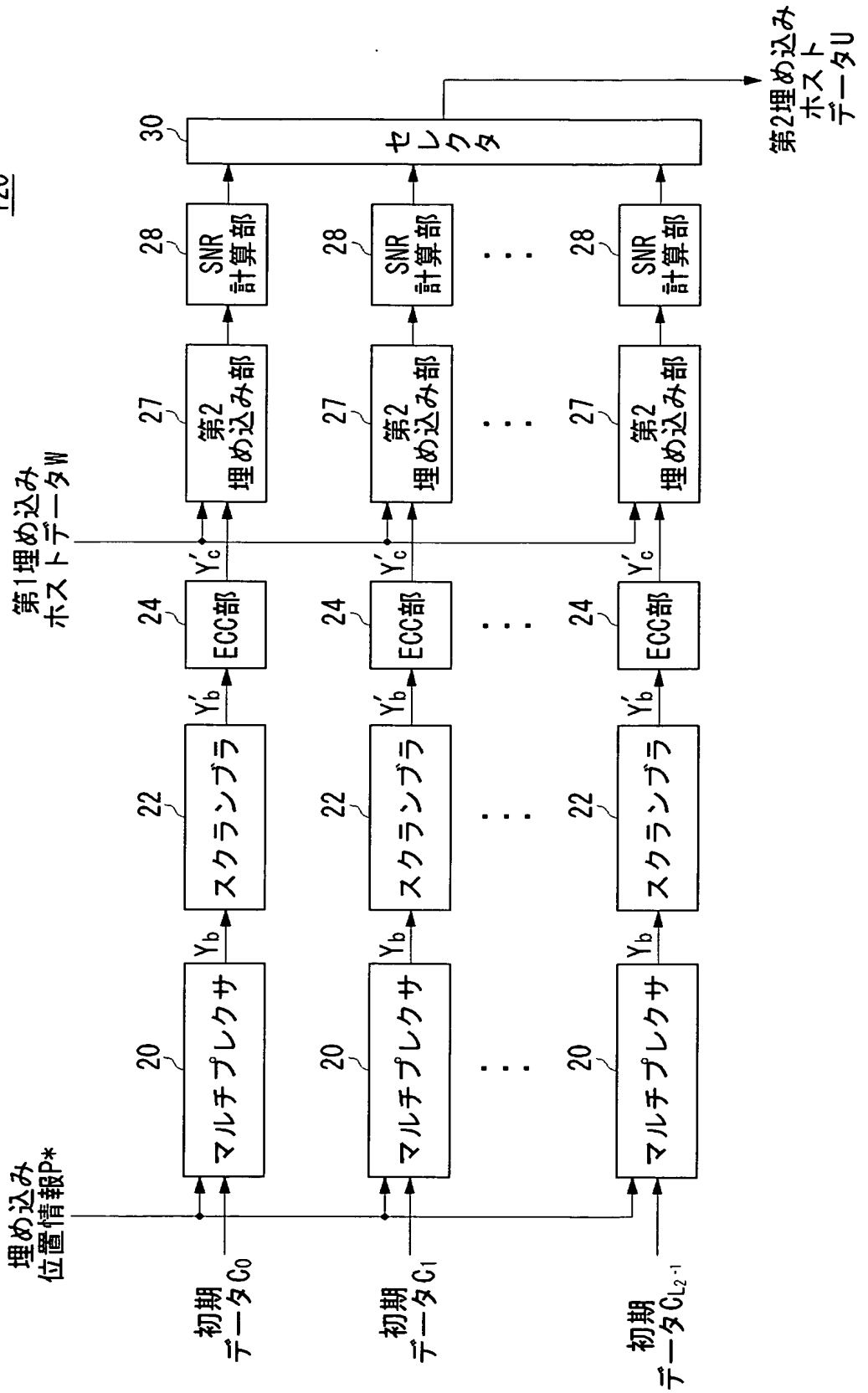
【図５】


100
110
第1透かし埋め込みブロック
暗号化部
10
位置検出部
12
X
P
第1透かし埋め込み部
14
W
120
第2透かし埋め込みブロック
変更部
16
P
Y'
第2透かし埋め込み部
18
第2埋め込みホストデータU
透かし情報I
ホストデータV
秘密鍵K

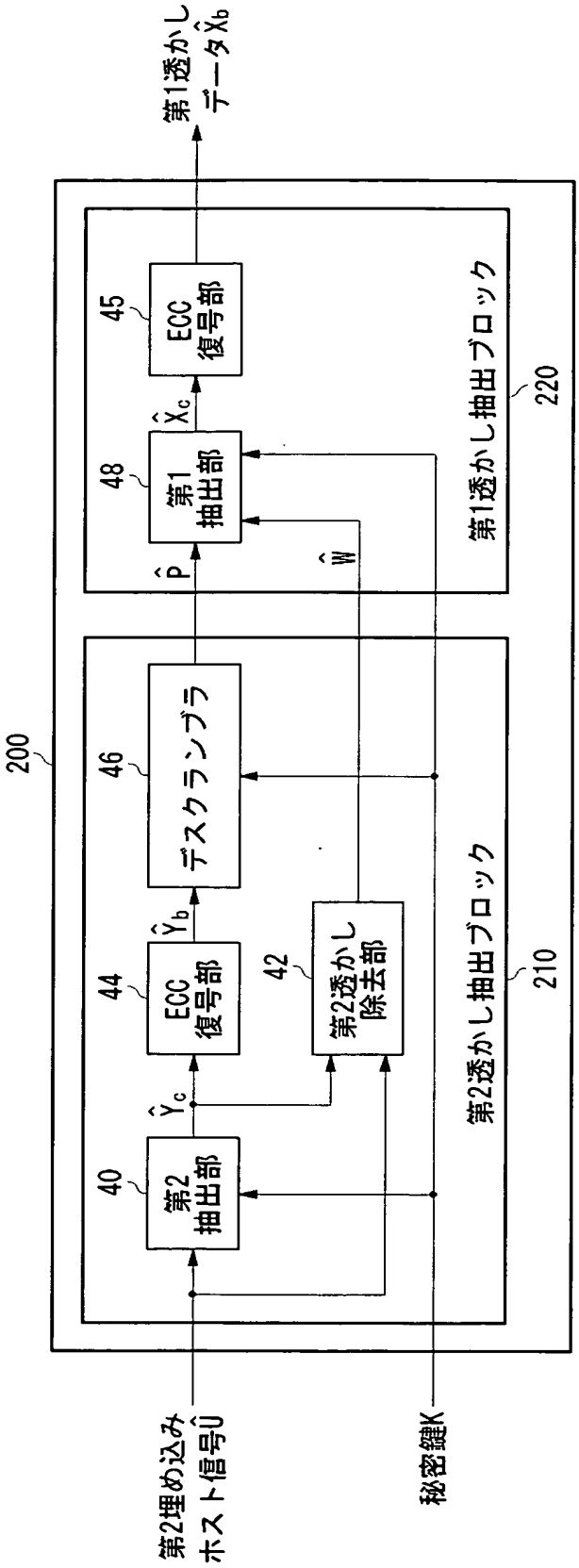
【図６】


110
32
セレクタ
第1埋め込みホストデータW
埋め込み位置情報P*
28
SNR計算部
26
第1埋め込み部
ホストデータV
Xc
P
24
ECC部
60
位置情報生成部
透かしデータX

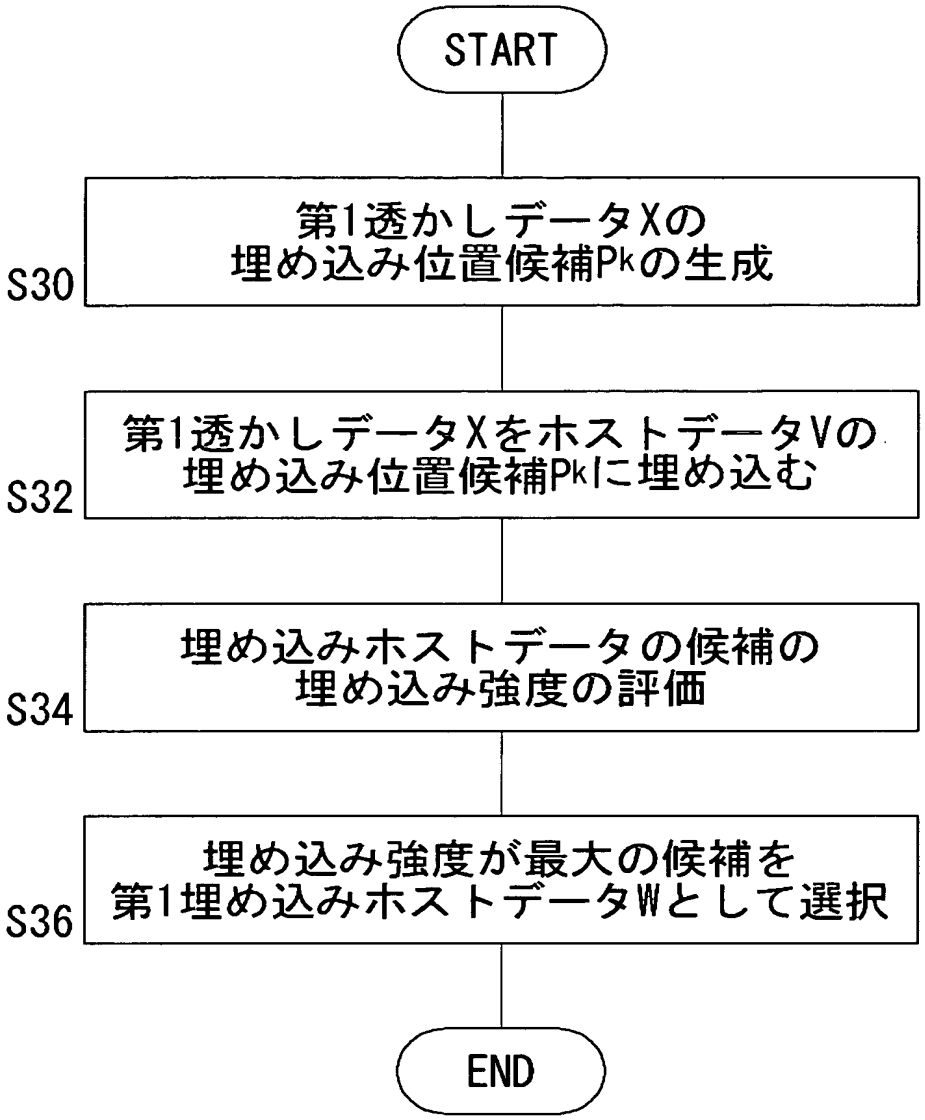
【図７】


120
埋め込み
位置情報P*
第1埋め込み
ホストデータW
初期
データC_0
初期
データC_1
初期
データC_{L_2-1}
マルチプレクサ
スクランブラ
ECC部
第2
埋め込み部
SNR
計算部
セレクタ
第2埋め込み
ホスト
データU
20
22
24
27
28
30
Y_b
Y'_b
Y'_c

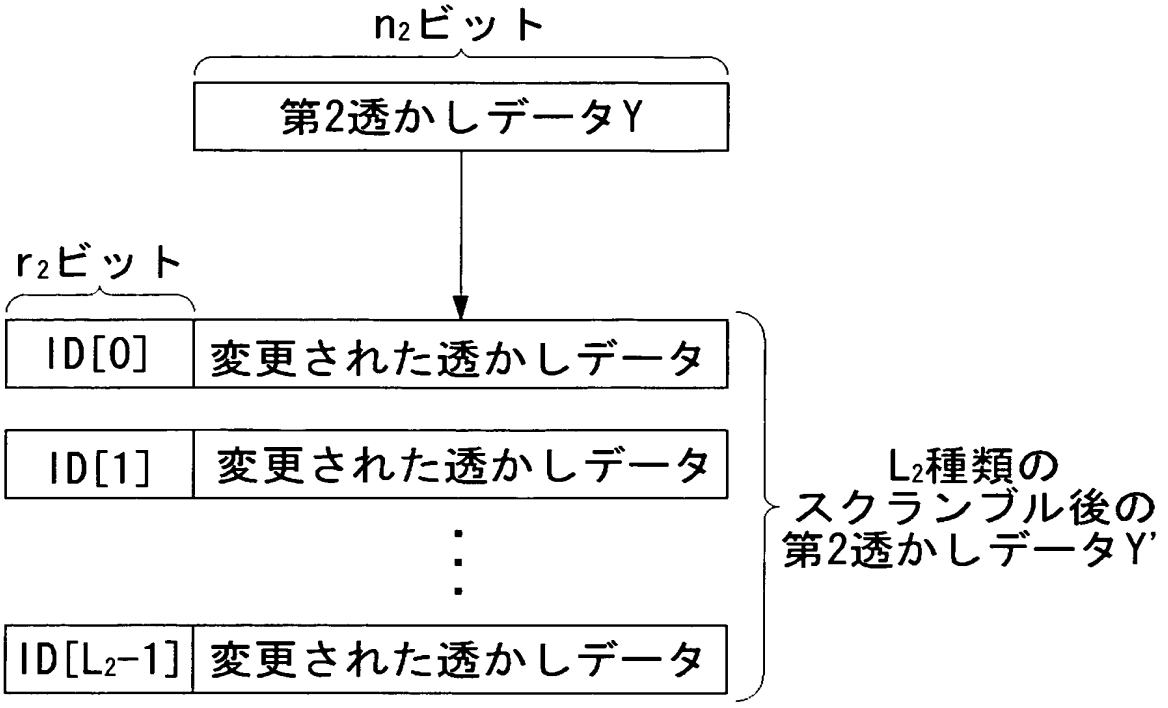
【図８】


第1透かしデータ $\hat{X}_b$
200
第1透かし抽出ブロック
220
第2透かし抽出ブロック
210
45
ECC復号部
48
第1抽出部
46
デスクランブラ
44
ECC復号部
42
第2透かし除去部
40
第2抽出部
$\hat{X}_c$
$\hat{P}$
$\hat{W}$
$\hat{Y}_b$
$\hat{Y}_c$
第2埋め込みホスト信号$\hat{U}$
秘密鍵K

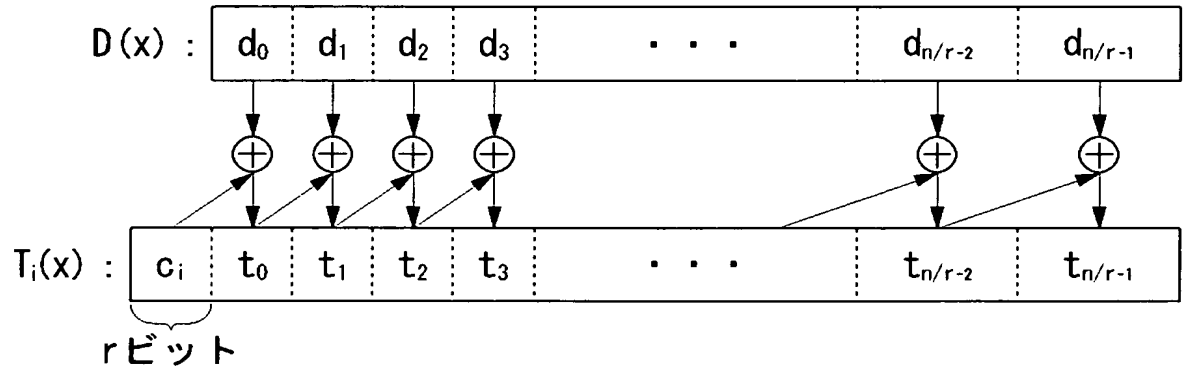
【図９】


START
S30
第1透かしデータXの
埋め込み位置候補Pkの生成
S32
第1透かしデータXをホストデータVの
埋め込み位置候補Pkに埋め込む
S34
埋め込みホストデータの候補の
埋め込み強度の評価
S36
埋め込み強度が最大の候補を
第1埋め込みホストデータWとして選択
END

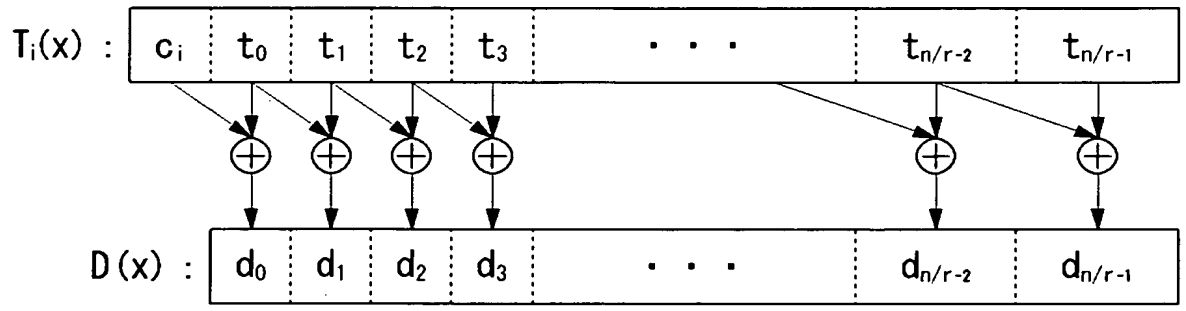
【図１０】


n2ビット
第2透かしデータY
r2ビット
ID[0]
変更された透かしデータ
ID[1]
変更された透かしデータ
ID[L2-1]
変更された透かしデータ
L2種類の
スクランブル後の
第2透かしデータY'

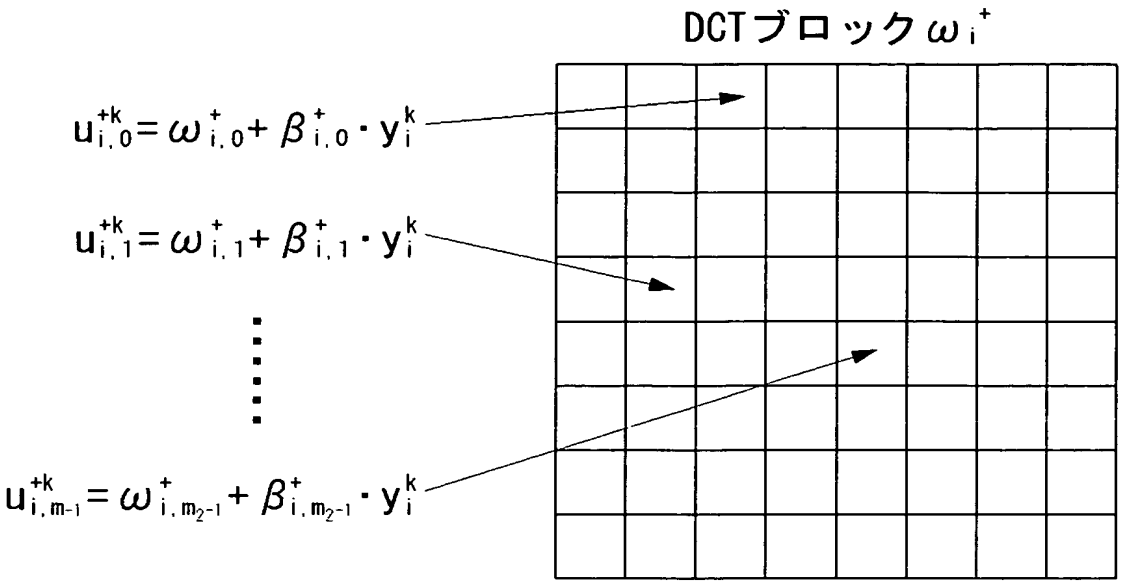
【図１１】


D(x) :
d0 d1 d2 d3 ・・・ dn/r-2 dn/r-1
Ti(x) :
ci t0 t1 t2 t3 ・・・ tn/r-2 tn/r-1
rビット

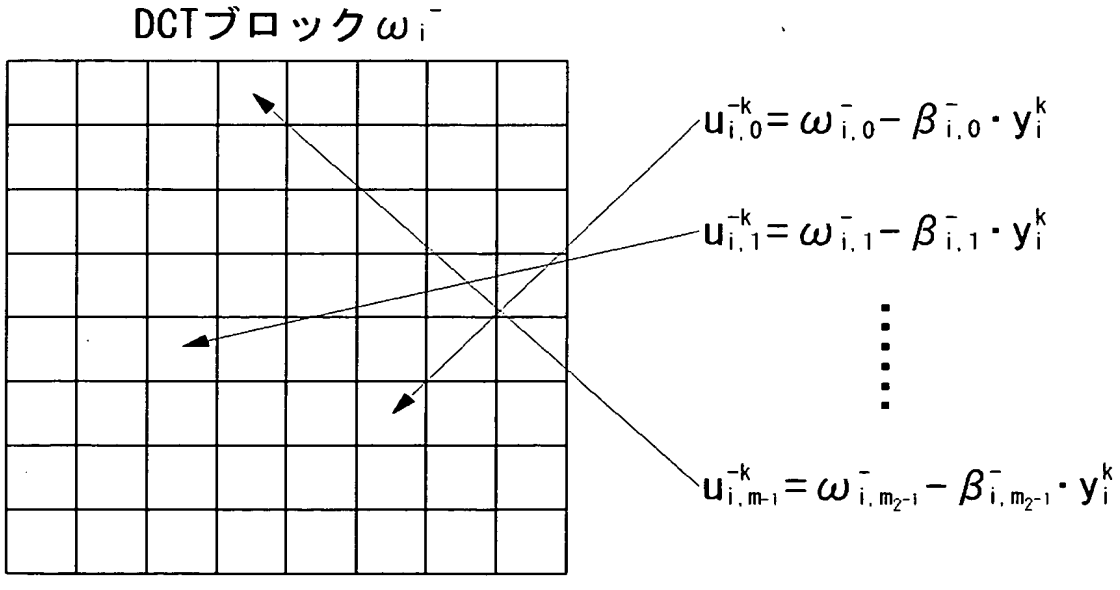
【図１２】


Ti(x) :
ci t0 t1 t2 t3 ・・・ tn/r-2 tn/r-1
D(x) :
d0 d1 d2 d3 ・・・ dn/r-2 dn/r-1

【図１３】

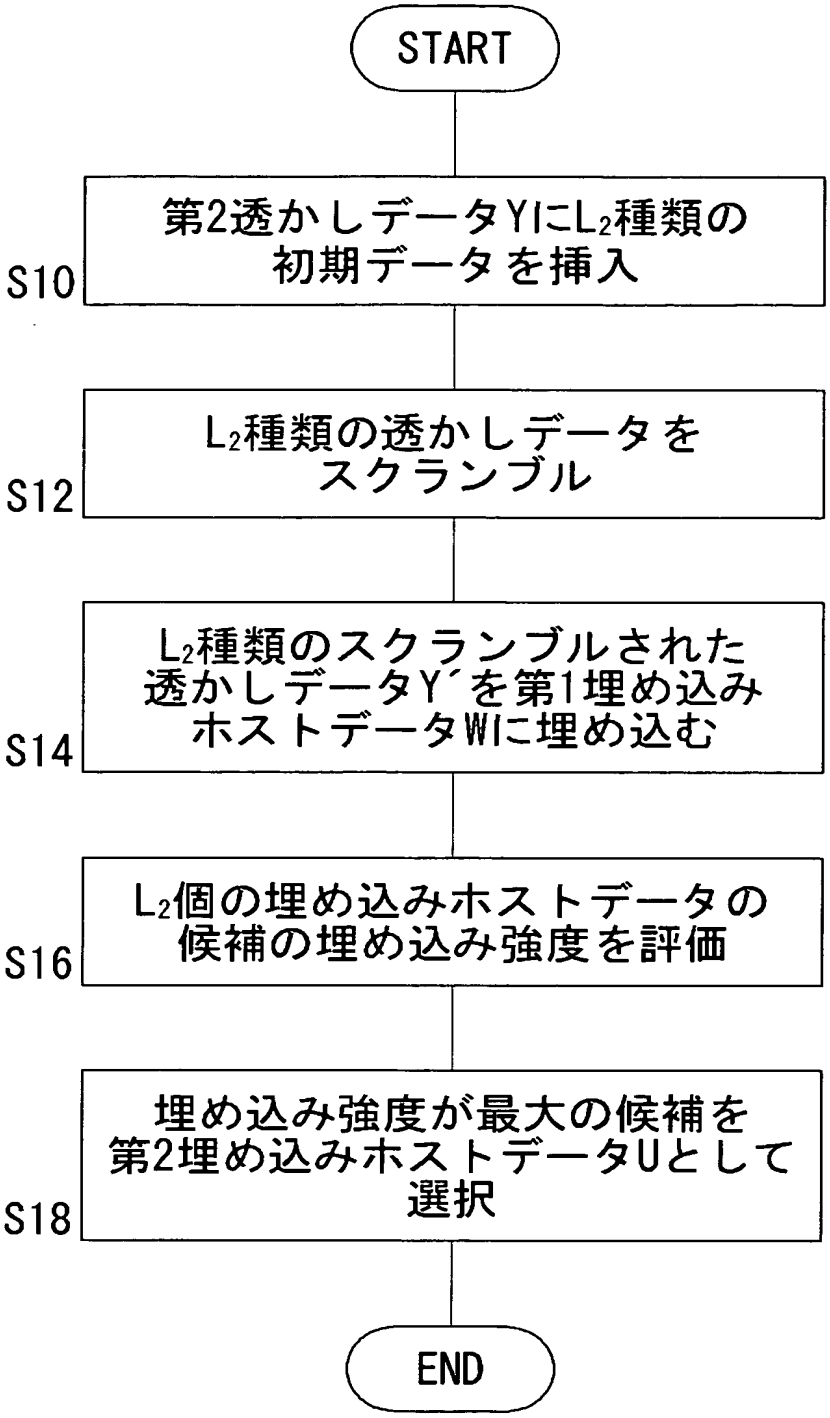

DCTブロックω_i^+
$u_{i,0}^{+k}=\omega_{i,0}^{+}+\beta_{i,0}^{+}\cdot y_i^k$
$u_{i,1}^{+k}=\omega_{i,1}^{+}+\beta_{i,1}^{+}\cdot y_i^k$
$u_{i,m-1}^{+k}=\omega_{i,m_2-1}^{+}+\beta_{i,m_2-1}^{+}\cdot y_i^k$

(a)

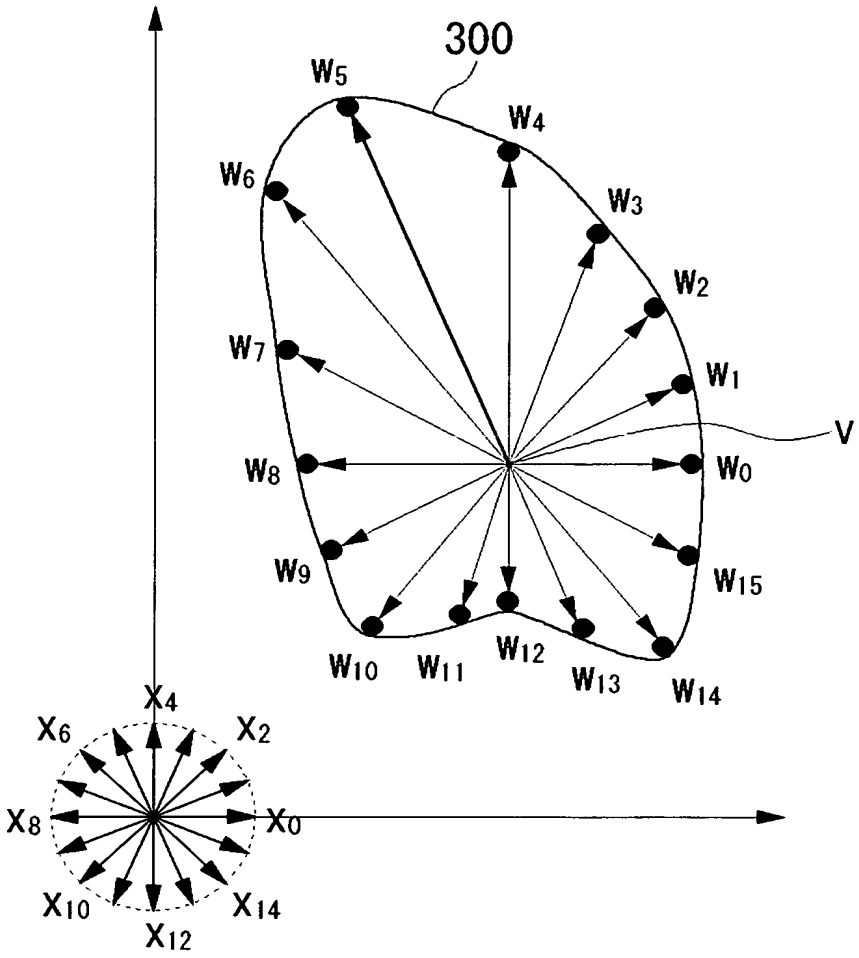

DCTブロックω_i^-
$u_{i,0}^{-k}=\omega_{i,0}^{-}-\beta_{i,0}^{-}\cdot y_i^k$
$u_{i,1}^{-k}=\omega_{i,1}^{-}-\beta_{i,1}^{-}\cdot y_i^k$
$u_{i,m-1}^{-k}=\omega_{i,m_2-1}^{-}-\beta_{i,m_2-1}^{-}\cdot y_i^k$

(b)

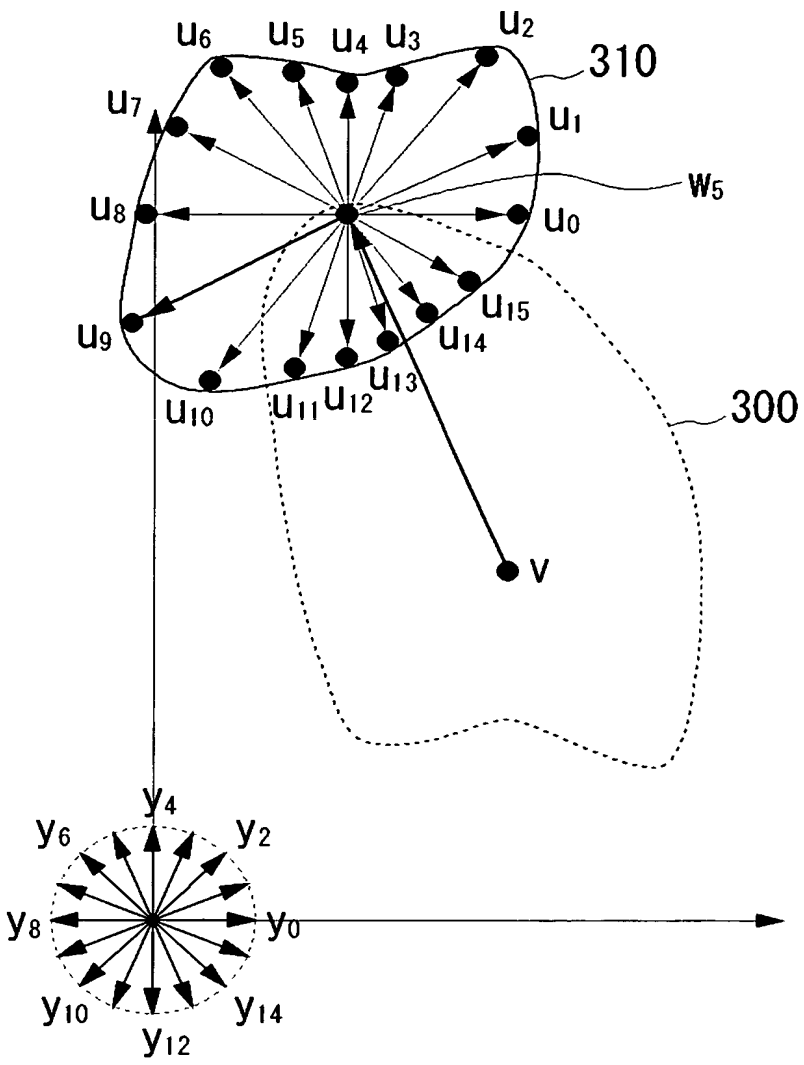
【図１４】


START
S10
第2透かしデータYにL2種類の初期データを挿入
S12
L2種類の透かしデータをスクランブル
S14
L2種類のスクランブルされた透かしデータY´を第1埋め込みホストデータWに埋め込む
S16
L2個の埋め込みホストデータの候補の埋め込み強度を評価
S18
埋め込み強度が最大の候補を第2埋め込みホストデータUとして選択
END

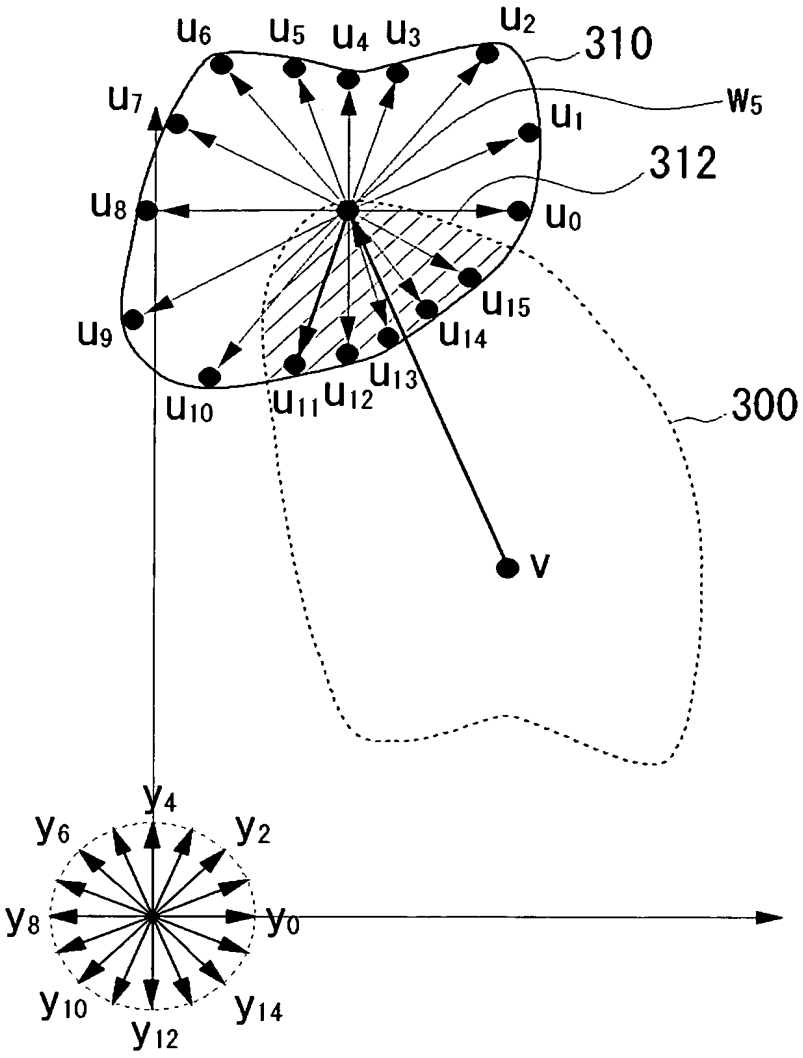
【図１５】


300
W5
W4
W6
W3
W2
W7
W1
V
W8
W0
W9
W15
W10
W11
W12
W13
W14
X4
X6
X2
X8
X0
X10
X14
X12

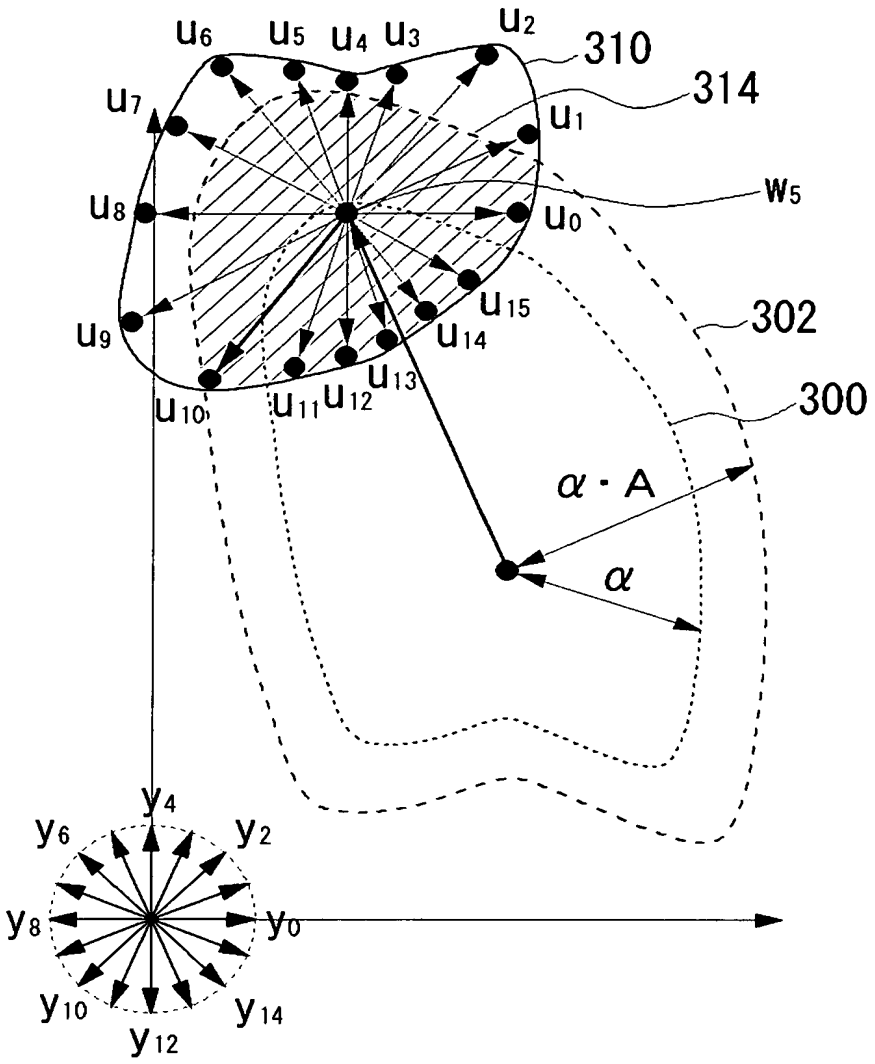
【図１６】


u6
u5
u4
u3
u2
310
u7
u1
w5
u8
u0
u15
u9
u14
u13
u10
u11
u12
300
v
y4
y6
y2
y8
y0
y10
y14
y12

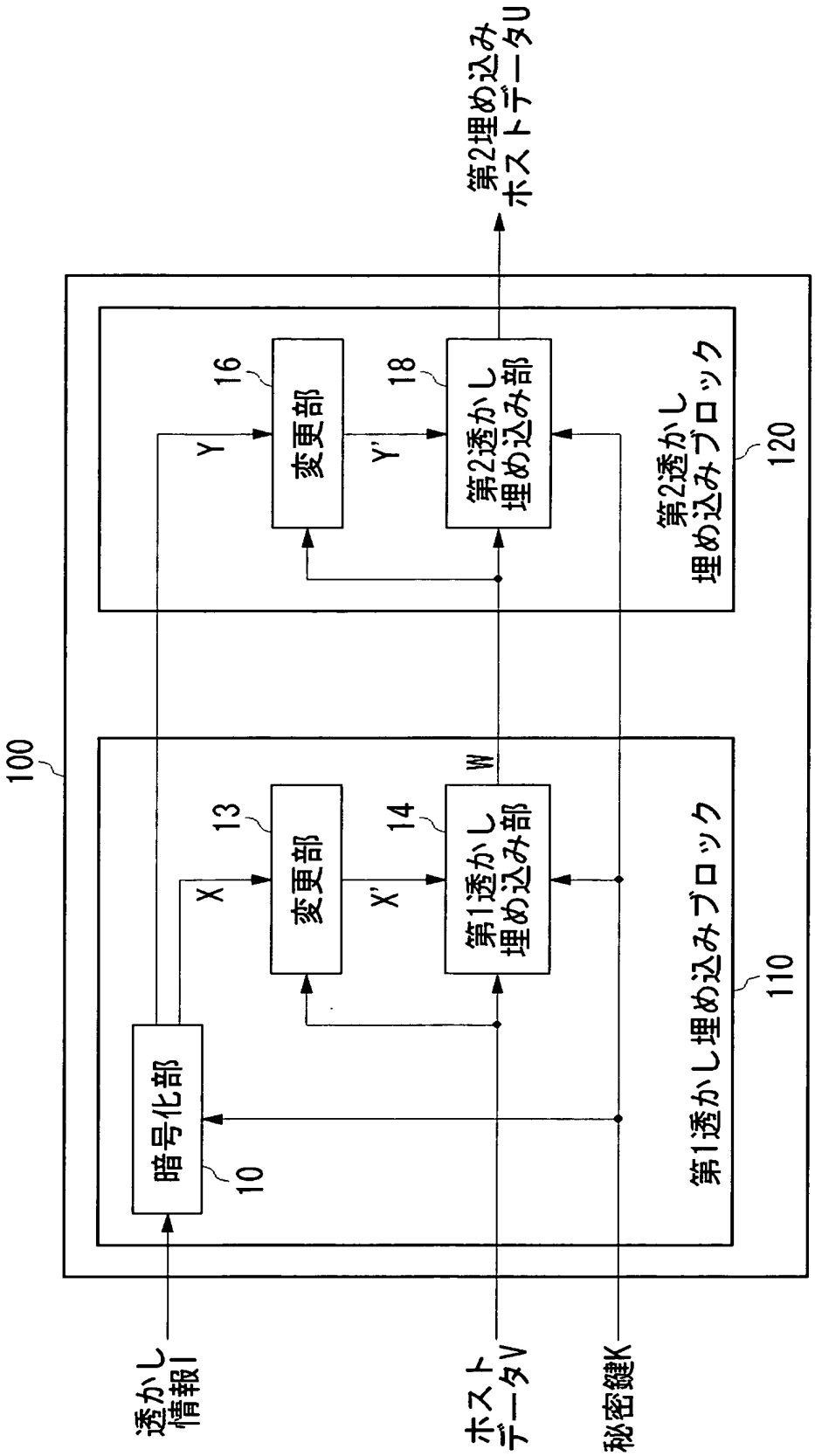
【図１７】


u6
u5
u4
u3
u2
310
u7
w5
u1
312
u8
u0
u15
u9
u14
u13
u10
u11
u12
300
v
y4
y6
y2
y8
y0
y10
y14
y12

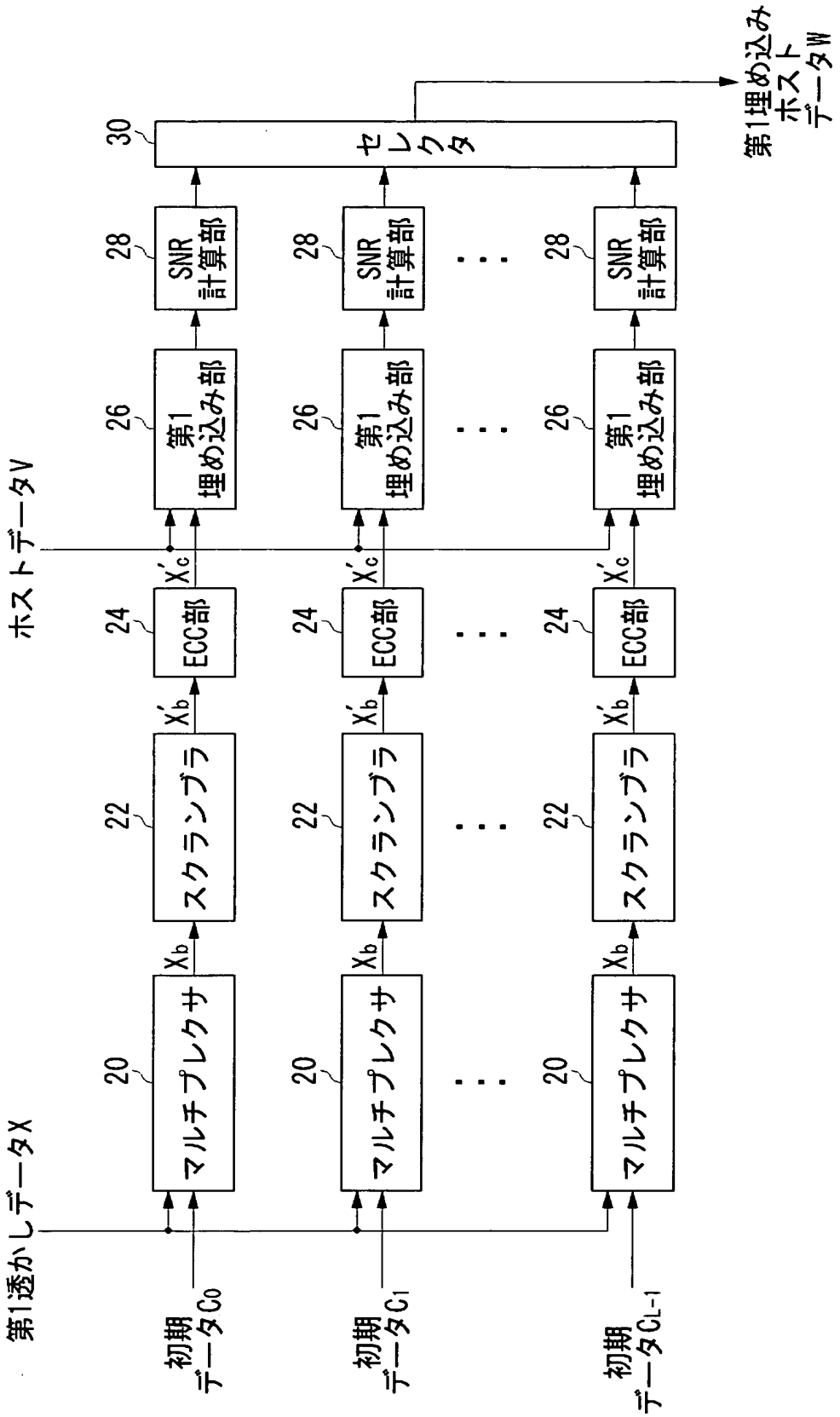
【図１８】


u6
u5
u4
u3
u2
310
314
u7
u1
w5
u8
u0
u15
302
u9
u14
u13
u10
u11
u12
300
α・A
α
y4
y6
y2
y8
y0
y10
y14
y12

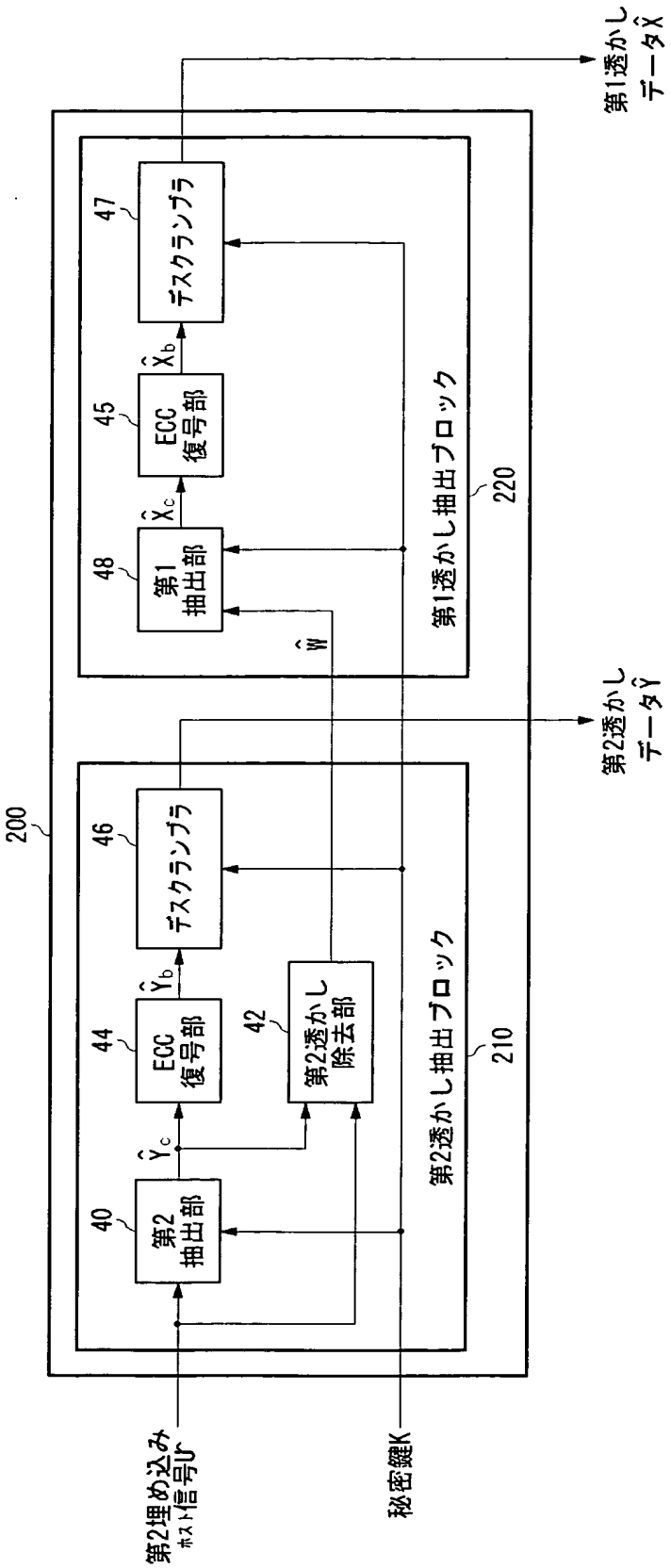
【図１９】


第2埋め込み
ホストデータU
16
18
Y
変更部
Y'
第2透かし
埋め込み部
第2透かし
埋め込みブロック
120
100
W
13
14
X
変更部
X'
第1透かし
埋め込み部
暗号化部
10
第1透かし埋め込みブロック
110
透かし
情報I
ホスト
データV
秘密鍵K

【図２０】


110
第1透かしデータX
ホストデータV
第1埋め込みホストデータW
初期データC_0
初期データC_1
初期データC_{L-1}
20 マルチプレクサ
22 スクランブラ
24 ECC部
26 第1埋め込み部
28 SNR計算部
30 セレクタ
X_b
X'_b
X'_c

【図２１】


200
第1透かしデータ $\hat{X}$
第2透かしデータ $\hat{Y}$
第1透かし抽出ブロック
220
47
デスクランブラ
45
ECC復号部
$\hat{X}_b$
48
第1抽出部
$\hat{X}_c$
$\hat{W}$
第2透かし抽出ブロック
210
46
デスクランブラ
44
ECC復号部
$\hat{Y}_b$
42
第2透かし除去部
40
第2抽出部
$\hat{Y}_c$
第2埋め込みポスト信号U
秘密鍵K

【書類名】　　要約書

【要約】

【課題】　電子透かしの耐性を強化し、透かしの検出精度を改善するのは難しい。

【解決手段】　第１透かし埋め込みブロック１１０において、位置検出部１２は、第１透かしデータＸの複数の埋め込み位置Ｐの候補を生成し、第１透かし埋め込み部１４は、ホストデータＶのそれらの埋め込み位置Ｐの候補に第１透かしデータＸを埋め込み、透かしの耐性が強い第１埋め込みホストデータＷを選択して出力する。第２透かし埋め込みブロック１２０において、変更部１６は、第１透かしデータＸの埋め込み位置Ｐに関する情報をスクランブルして複数の第２透かしデータＹ’の候補を生成し、第２透かし埋め込み部１８は、それらの候補を第１埋め込みホストデータＷに埋め込み、耐性の強い第２埋め込みホストデータＵを選択して出力する。

【選択図】　　図５

特願２００２－３２５８９６

出　願　人　履　歴　情　報

識別番号　　［０００００１８８９］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　　新規登録
住　所　　大阪府守口市京阪本通２丁目１８番地
氏　名　　三洋電機株式会社

２．変更年月日　　１９９３年１０月２０日
［変更理由］　　住所変更
住　所　　大阪府守口市京阪本通２丁目５番５号
氏　名　　三洋電機株式会社